Insight takes a page from its own playbook and adopts Microsoft 365 E5 as its global security platform

Insight's journey as a large enterprise adopting E5 is relevant to all businesses looking to mature their cybersecurity operations.

Background

Supply chain attack risks – highlighted by the SolarWinds event in December 2020 – along with the risks associated with open-source libraries, such as the Java Log4j vulnerability issue in December 2021, prompted Insight to rethink its overall security program and cybersecurity operations toolset. The maturity of our security teammates and integration with current tooling were heavily considered with an emphasis on protecting our endpoints, visibility, correlation, incident response, and remediation. Building a solution that consisted of existing best-of-breed tools was an "in fashion" option, but time constraints and the integration that this approach would require swayed Insight to the platform approach. Additional considerations included the ability to monitor both on-premises and cloud resources, as well as the ability to add capabilities as our team and needs matured.

Why we chose Microsoft 365 E5

The choice for Insight to upgrade from our Microsoft 365™ E3 licensing plan to Microsoft 365 E5 was primarily based on security. E5's security capabilities met all our immediate needs and gave us room to grow, while additional features brought supplemental value to our current collaboration and voice solutions.

For the uninitiated, Microsoft 365 E5 includes a diverse set of cybersecurity capabilities:

Microsoft Defender XDR	Microsoft Defender for Cloud Apps	Microsoft Defender for Office 365	Microsoft Purview	Microsoft Defender for Identity	Advanced Microsoft Entra ID features	Microsoft Defender for Endpoint

Upgrading from E3 to E5 is a non-trivial amount of spend per teammate, so we engaged in the appropriate due diligence comparing many other security platforms and their total cost of ownership along with associated coverage and integration concerns. In the end, Microsoft 365 E5 was the clear winner. With the support of our executive team and board, we committed to executing the upgrade and using the platform to protect our brand, teammates, clients, and partners – as a part of a bigger effort to prevent fires rather than fight them.

What our leaders have to say...

James Morgado, CFO –

"We traded multiple products and services for a single platform that delivers value back to the organization. After considering all that it includes and our team's ability to use those features effectively, we believe it has been a smart investment."

Don Quigley, Director of Information Security –

"We engaged Microsoft at a time when their platform was rapidly maturing and adding features. In the end, it gave us more product integrations and features but there was much our team had to adapt to during the times of console and name changes. I feel like things have stabilized now."

Jason Rader, CISO –

"We were very early adopters of many of the features of the platform, including Sentinel, Defender, Purview, and Security Copilot to name a few. In some cases, we had to blaze a trail, but that makes the path easier for those who come after us as we share our lessons learned."

Joyce Mullen, President & CEO –

"Cybersecurity is not something a Fortune 500 company can compromise on. Our selection of Microsoft's security platform was all about our team's ability to leverage the platform to protect our assets and brand."

Microsoft 365 E5 global security platform

Our approach

Once the acquisition of the licensing and entitlement was complete, the real work began. As you might imagine, it takes time to incorporate a new platform, migrate from previous systems, and operationalize new features.

These were the key steps in our deployment and adoption:

- Defined initial policies to govern authentication, email filtering, endpoint security posture, Data Loss Prevention (DLP), and data classification
- Deployed the Defender for Endpoint agents to all devices to replace existing Endpoint Detection and Response (EDR) solution
- Implemented Microsoft Sentinel as our Security Information and Event Management (SIEM) system and configured logging retention from 90 days to one year to increase visibility and correlate low and slow tactics
- Set explicit and risk-based Conditional Access policies to only allow specific users and machines access to internal resources
- Immediately instituted SMS-based Level 1 Multi-Factor Authentication (MFA) for all users worldwide and gradually, based on user acceptance, increased to phishing-resistant MFA for all teammates using the Authenticator App and Passkeys
- Increased coverage with Defender for Servers (both Linux® and Windows®)
- Added Defender for Identity sensors to all domain controllers
- Used Microsoft Purview to label and protect data on corporate SharePoint® sites
- Enabled data sharing between the various Advanced Threat Detection components and the Defender XDR console to aggregate signals and detection data
- Automated security workflows and correlations leveraging the AI capabilities of Security Copilot
- Leveraged built-in assessment tools (IT phishing) to ensure best practices
- Continued to iteratively enhance policies, broaden coverage, and manage false positives so alerts are of higher quality

Benefits and outcomes

Insight's investment in Microsoft's security platform including Microsoft 365 E5 has been impactful. Access to highly capable technology, along with a dedicated team, has been instrumental in driving innovation, efficiency, and competitive advantage – empowering Insight to tackle complex challenges and remain confident in our overall security posture. This has enabled not only the transformation of Insight's security team but also the security to assist in the transformation of Insight as a whole.

A final word

Security isn't easy, and Insight's journey is unique to our company. There is a myriad of variables related to your current technology stack or company culture that would make your journey completely different. It is always best to have a trusted partner to help you navigate the current offerings and obstacles.

Lessons learned

Do your homework.

Understand the impact on the business and users of the security component you are implementing. A hasty launch of even the best technology can create a situation that causes skepticism and questions about the value of security. Be consultative with the business.

Get trained and get help.

Insight's internal security team engaged with Insight's client-facing security consultants to navigate the influx of new capabilities and integrations. This ensured the success of Insight's rollout and provided access to seasoned professionals who were comfortable with the newest features in the Microsoft platform.

Outsource security elements that add no value to your team.

Don't be hesitant to enlist help from a Managed Services provider. At Insight, we consume the same Managed XDR services that we offer our clients. This gives us 24/7 coverage, access to the latest tech stack, and a wealth of skillsets.

Sharpen the saw.

There are so many aspects to Microsoft's platform that it's easy to miss something on your first pass. Go back, validate settings, and look for new features that are constantly being added. These steps can greatly enhance your security posture.

Microsoft 365 E5 global security platform

E3 vs. E5

		Microsoft 365 E3	Microsoft 365 E5
Microsoft 365 Enterprise E5 (includes E3 solutions)	**Identity and Access Management**	· Microsoft Entra ID P1 · Windows Hello® · Credential Guard	· Microsoft Entra ID P2
	Information Protection	· Azure® Information Protection P1 · Office 365® DLP · Windows Information Protection · BitLocker®	· Azure Information Protection P2 · Microsoft Cloud App Security · Office 365 Cloud App Security
	Threat Protection	· Microsoft Advanced Threat Analytics · Windows Defender Antivirus · Device Guard	· Windows Defender Advanced Threat Protection · Office 365 Advanced Threat Protection · Office 365 Threat Intelligence · Azure Advanced Threat Protection
	Security Management	· Secure Score · Microsoft Security and Compliance Center · Windows Security Center	· Additional management reports and capabilities
	Compliance	· eDiscovery	· Advanced eDiscovery, Customer Lockbox, Advanced Data Governance
	Analytics	· Delve	· Power BI® Pro, MyAnalytics
	Productivity, Creativity, and Teamwork solutions	· Office Applications · Outlook/Exchange · Microsoft Teams®, Skype for Business	· Skype Audio Conferencing · Phone System

		Microsoft 365 E3	Microsoft 365 E5
Threat Protection	Microsoft Advanced Threat Analytics, Device Guard, Credential Guard, AppLocker, Enterprise, Data Protection	✓	✓
	Microsoft Defender for Office 365	✗	✓
	Microsoft Defender for Endpoint	✗	✓
	Office 365 Threat Intelligence	✗	✓
Identity Management	Self-service password reset for hybrid Microsoft Entra ID accounts, Azure MFA, Conditional Access	✓	✓
	Microsoft Entra ID: Cloud App Discovery, Microsoft Entra ID Connect Health, SSO for more than 10 apps	✓	✓
	Microsoft Entra ID Plan 2	✗	✓
Device & App Management	Microsoft Intune®, Windows AutoPilot	✓	✓
	Windows Virtual Desktop	✓	✓
	Shared computer activation	✓	✓
	Microsoft Desktop Optimization Pack, VDA	✓	✓
Information Protection	Microsoft DLP, Azure Information Protection Plan 1	✓	✓
	Azure Information Protection Plan 2, Microsoft Cloud App Security, Office 365 Cloud App Security	✗	✓