efex
SMARTER TECH FOR AMBITIOUS BUSINESS

Managed Cyber

Next level protection & IT support for every business

Inclusions	Managed Cyber Zero	Managed Cyber Essentials	Managed Cyber Premium	Managed Cyber Apex
Remote monitoring & management	✓	✓	✓	✓
Endpoint detection & response	✓	✓	✓	✓
Ransomware detection & response	✓	✓	✓	✓
Anti-virus software	Standard	Advanced	Advanced	Advanced
Advanced email phishing defence & spam filtering	✓	✓	✓	✓
Server uptime monitoring	✓	✓	✓	✓
Windows Operating System software updates	✓	✓	✓	✓
3rd party software updates	Core	Standard	Advanced	Advanced
Uninterrupted Power Supply (UPS) alerts management	✓	✓	✓	✓
Vulnerability scanning	✓	✓	✓	✓
M365 licence management & security baseline	✓	✓	✓	✓
Daily M365 backup	✓	✓	✓	✓
M365 self-service password resets		✓	✓	✓
Microsoft Intune support		✓	✓	✓
System & performance monitoring		✓	✓	✓
Monthly M365 reporting		✓	✓	✓
Phishing training		✓	✓	✓
Dark web ID monitoring		Standard	Standard	Advanced
Domain Name System (DNS) filtering for malicious/unauthorised websites		Standard	Advanced	Advanced
Security Operations Centre (SOC) for M365 tenant		✓	✓	✓
Security Operations Centre (SOC) for endpoints & servers			✓	✓
Advanced SOC / Security Information & Event Management (SIEM)			Add on	✓
Advanced conditional access			✓	✓
Application whitelisting			✓	✓
Copilot & advanced workflow support			✓	✓
Incident response & problem management			✓	✓
Essential 8 gap analysis assessment & report			Add on	✓
Digital footprint monitoring			Add on	Add on
Quarterly penetration testing			Add on	Add on
Phishing simulations				✓
Monthly cyber reporting				✓
Technology roadmapping				✓
Phishing resistant / FIDO2 compliant Multifactor Authentication				Add on
Microsoft 365 hardening				Add on
Advanced vulnerability scannning				Add on
Price per user / month including helpdesk support	**$60**	**$120**	**$180**	**$280**

efex
SMARTER TECH FOR AMBITIOUS BUSINESS

Managed Cyber

Next level protection & IT support for every business

Inclusion	What is it?	What does it do?	The outcome you can expect
Remote monitoring & management	A technology tool set that's permanently integrated with individual devices	Acting as a silent guardian, it continuously monitors system health, performance, and security status in real time. It ensures each device receives timely software updates and security patches, reducing vulnerabilities without interrupting the user's workflow. This proactive approach helps prevent issues like malware infections, system crashes, or performance slowdowns before they impact productivity.	Fewer disruptions, faster issue resolution, and stronger data security, all while enabling staff to stay productive and focused on their work.
Endpoint detection & response	A technology tool set that's permanently integrated with individual devices	Provides each device with intelligent, real-time protection against advanced cyber threats. From the endpoint's perspective, efex is constantly watching for unusual behaviour, such as unauthorised access attempts or suspicious file activity, and can take immediate action to stop threats in their tracks. Using advanced behavioural analysis and memory scanning, it detects both known and unknown attacks, including zero-day exploits and fileless malware. This means your devices are not only shielded from traditional viruses but also from sophisticated, evolving threats - all without disrupting the user's experience.	Sensitive data is kept safe and operations continue to run smoothly. The risk of costly breaches, downtime, or data loss is dramatically reduced with this depth of protection.
Ransomware detection & response	A technology tool set that's permanently integrated with individual devices	In real-time, it actively monitors for signs of ransomware activity—such as rapid file encryption or abnormal system behaviour—and responds instantly to stop the threat. From the device's point of view, it's like having a built-in security expert that can detect and block ransomware before it causes serious damage. If an attack is detected, the system can automatically isolate the device from the network, halt malicious processes, and initiate recovery protocols—all without user intervention.	If ransomware slips past traditional defenses, the endpoint remains protected, minimising data loss, downtime, and disruption to the business.
Anti-virus software	Software that lives on individual devices	Uses advanced AI and behavioural analysis to detect and block threats in real time. Acting as a vigilant security layer at the endpoint, it continuously scans for viruses, malware, and suspicious activity—without disrupting the user's workflow. Unlike traditional antivirus tools that rely solely on known threat signatures, it proactively identifies and neutralises emerging threats before they cause harm. Malicious files are automatically quarantined, threats are neutralised, and systems remain secure and productive with minimal user involvement. Every device in your organisation is protected around the clock, ensuring seamless defense against both known and evolving cyber threats.	A reduction in the risk of data breaches, downtime, and costly IT disruptions, while allowing employees to work confidently and productively.
Advanced email phishing defence & spam filtering	An AI-powered security layer embedded directly into each user's inbox	Provides an intelligent, always-on security layer that protects inboxes from phishing scams, impersonation attacks, and spam. Using AI-driven analysis and advanced threat detection, it continuously scans email content, sender behaviour, and historical patterns to block malicious emails before they reach users. Built on leading platforms like Microsoft Defender for Office 365, it filters junk and bulk messages, adapting to user feedback and global threat intelligence.	A cleaner, safer inbox with fewer distractions and a significantly reduced risk of falling for malicious emails—all while maintaining a seamless and productive email experience.
Server uptime monitoring	Cloud-based software that's integrated with the server	Acts as a real-time health monitor for each server, constantly tracking performance metrics like CPU usage, memory load, disk space, and network connectivity to ensure the system stays online and responsive. From the server's point of view, it's like having a 24/7 watchdog that immediately detects and reports any signs of downtime or performance issues, allowing for rapid intervention before users or business operations are affected.	Fewer disruptions, improved service availability, and greater confidence in your IT systems.Unexpected outages are prevented, risk of data loss is reduced, and critical services remain available, creating a stable, resilient IT environment that supports seamless business continuity.
Windows Operating System software updates	Cloud-based software that's integrated with each Windows device	Ensures Windows devices are always up to date with the latest security and performance updates. Functioning like a built-in maintenance assistant it quietly checks for approved patches, downloading them during off-peak hours, and applying them without disrupting the user's workflow. It ensures critical vulnerabilities are addressed promptly, system performance is optimised, and compliance is maintained. It also intelligently manages reboots, schedules, and exceptions.	Each device remains secure and stable without requiring manual oversight or user intervention. Updates are applied during scheduled windows (usually after hours) to avoid disrupting daily operations.
3rd party software updates	System maintenance deployment tool	Ensures every endpoint in your business—whether it's a desktop, laptop, or server—stays up to date with the latest versions of commonly used applications like Adobe Reader, Zoom, Chrome, and hundreds more. Software updates are applied automatically and silently in the background, minimising disruption. Risks associated with outdated software are eliminated, such as security vulnerabilities, performance issues, and compatibility problems. It also prevents "configuration drift," where different devices end up running different versions of the same application, which can lead to support headaches and inconsistent user experiences.	A consistent, secure, and professionally maintained software environment. Endpoints stay protected, compliant, and optimised, reducing cyber risks and ensuring system stability.
Uninterrupted Power Supply (UPS) alerts management	System monitoring tool	efex's UPS Alerts Management adds a vital layer of resilience to the IT environment, helping businesses maintain uptime, protect assets, and avoid costly disruptions. It ensures critical power infrastructure, like UPS is actively monitored to protect endpoints and servers from unexpected shutdowns or power-related failures. Endpoints & user devices are safeguarded against data loss and hardware damage caused by sudden power interruptions. efex's system continuously tracks the health, battery status, and connectivity of UPS units, and immediately generates alerts if any issues arise—such as low battery, communication failures, or power anomalies. These alerts are automatically prioritised and routed for action, ensuring potential problems are addressed before they impact users.	Greater protection for servers, workstations, and network equipment, reducing the risk of data loss, hardware damage, or costly downtime caused by sudden power outages. It also supports business continuity by ensuring systems can shut down gracefully or switch to backup power when needed. For users it's a seamless experience: their work remains uninterrupted, and their data stays safe, even during power fluctuations.
Vulnerability scanning	Security management tool	Provides continuous, behind-the-scenes protection for endpoints by identifying weaknesses in operating systems, installed software, and device configurations that could be exploited by cyber threats. User devices are regularly and silently scanned for known vulnerabilities—such as outdated software versions, missing patches, or insecure settings—without interrupting their work. efex's scanning engine compares each system against a vast and constantly updated database of known vulnerabilities (CVEs), flagging any issues that could pose a risk. When a vulnerability is detected, efex prioritises it based on severity and potential impact, allowing for swift remediation before it can be exploited.	A safer, more stable computing experience for all users, and all devices remain compliant, secure, and resilient against evolving cyber threats.
Microsoft 365 licence management	Cloud-based administrative tool	Enables full visibility and control over your Microsoft 365 environment without the complexity of managing it internally, ensuring every user has the right tools for their role. It continuously monitors usage and aligns license types with actual user needs. From timely onboarding new employees with the correct tools to reallocating unused licenses and managing renewals, every licence is accounted for to ensure it's delivering value.	The right users have the right licenses, so there's no risk of overspending or underutilising resources. It also improves operational efficiency and compliance.

efex.com.au/managed-cyber

efex
SMARTER TECH FOR AMBITIOUS BUSINESS

Managed Cyber

Next level protection & IT support for every business

Inclusion	What is it?	What does it do?	The outcome you can expect
Microsoft 365 security baseline	Cloud-based administrative tool	Implements and enforces a Microsoft 365 security baseline to deliver standardised, best-practice security configurations across the M365 tenant. By enforcing consistent settings for identity protection, threat management, data governance, and device compliance, efex's M365 security baseline helps safeguard environments against cyber threats and misconfigurations, whilst allowing tailored adjustments to meet specific organisational needs.	Digital operations are safeguarded in a more secure, compliant, and resilient IT environment and Microsoft 365 tenant.
Daily M365 backup	Routine maintenance software	Automatically creates secure copies of emails, files, calendars, and configurations across your organisation's M365 cloud environment. It ensures data is protected from accidental deletion, cyber threats, and system failures, enabling fast recovery and business continuity with minimal disruption.	Ensures your business can quickly recover from data loss, maintaining continuity and reducing downtime. For employees, it provides a safer, more reliable work environment with fewer disruptions and greater confidence in data protection
Microsoft 365 self-service password resets	Cloud-based administrative tool integrated with Microsoft Entra ID	Allows users to securely reset or recover their own passwords without the need for IT intervention. This significantly reduces the need for them to log help desk tickets which improves productivity. Configuration & management of the self-service password reset feature across client environments ensures seamless integration with Microsoft 365. This includes setting up secure authentication methods—such as mobile verification, email or security questions—tailored to each organisation's policy requirements. This service is especially valuable for hybrid or remote workforces, offering users a consistent and localised password reset experience from any device, anywhere.	Businesses minimise downtime caused by account lockouts or forgotten credentials, while maintaining compliance and security standards.
Microsoft Intune support	Cloud-based technical support service	Streamlines deployment of applications, zero-touch provisioning, and centralised policy enforcement, ensuring every device - whether corporate-owned or BYOD, complies with security baselines and organisational policies, using conditional access and mobile application management to protect sensitive data without disrupting productivity. This includes proactive monitoring, patch management, and continuous optimisation aligned with Microsoft Secure Score and Centre for Internet Security (CIS) benchmarks. Software deployments are automated, security policies are enforced, and device health is monitored in real time, reducing IT overhead.	Properly configured, updated, and protected endpoints across your mobile or hybrid workforce, minimised downtime and support costs, and secure business data—even beyond the office network.
System & performance monitoring	Cloud-based IT management tool	Provides real-time visibility into the health and performance of every endpoint across your business via advanced remote monitoring and management. Whether it's a desktop, laptop, or server, system metrics like CPU usage, memory consumption, disk health, and network activity are continuously monitored. Each device is proactively observed for signs of performance degradation, potential hardware failures, or unusual behaviour that could indicate a security threat. Automated alerts and intelligent thresholds allow efex to respond swiftly to issues before they impact users, minimising downtime and maintaining optimal performance.	Business owners and managers don't need to worry about the technical details because efex handles everything behind the scenes. There are fewer unexpected disruptions, faster issue resolution, devices run smoothly, their lifespan is extended and user productivity is enhanced along with a more stable IT environment overall.
Monthly M365 reporting	Usage & security snapshot	Provides a structured overview of your organisation's M365 environment, including user activity, mailbox usage, security events, and compliance status. It highlights trends, anomalies, and risks like phishing attempts, malware detections, or inactive accounts. It also supports decision-making by surfacing actionable insights.	By monitoring performance t ensures policy alignment, and helps maintain operational transparency.
Phishing training	Digital education resource	Equips users with the knowledge and instincts to recognise and avoid phishing attacks through regular, interactive simulations and educational content. Users receive realistic, scenario-based phishing emails that mimic the tactics used by real cybercriminals, followed by immediate feedback and short, engaging training modules if they fall for the bait. These monthly exercises help users build awareness and sharpen their ability to spot red flags like suspicious links, urgent language, or spoofed sender addresses. Over time, this consistent exposure transforms employees into a strong first line of defense, reducing the likelihood of a successful phishing attack. For users, it's a low-pressure, educational experience that fits seamlessly into their workflow.	A significantly stronger cyber security posture because employees are more confident & capable of identifying threats before they cause harm. The risk of a data breach is reduced considerably along with the risk of financial loss.
Dark web identity monitoring	Security management tool	Working silently in the background to protect users, it continuously scans the dark web for signs that their personal or business credentials have been exposed. If their email address, passwords, or other sensitive information tied to their identity is found in a data breach or being traded on underground forums, efex will detect it and alert the appropriate contacts immediately. This early warning system gives users and businesses the chance to take swift action, like resetting passwords or enabling multi-factor authentication before cybercriminals can exploit the compromised data. It's a seamless layer of protection that doesn't require any action until a threat is detected, offering peace of mind that employee digital identities are being actively monitored and defended, even in the darkest corners of the internet.	Reduced financial risk associated with fraud and cyberattacks, better business continuity and a stronger cybersecurity posture.
Domain Name System (DNS) filtering for malicious/ unauthorised websites	Cloud-based security layer integrated with the network	Acts as a powerful first line of defense at the endpoint level, protecting users from online threats before they reach the device. Whether it's a laptop, desktop, or mobile device, every web request is automatically checked against a constantly updated database of malicious, suspicious, or inappropriate domains. If a user attempts to access a harmful site, such as one hosting malware, phishing scams, or ransomware, the connection is blocked instantly, preventing the threat from ever loading. This happens silently in the background, without slowing down the user's browsing experience. Content control is also enabled, allowing businesses to restrict access to non-work-related or high-risk websites, helping to maintain productivity and compliance. With real-time threat detection, AI-driven domain categorisation, and customisable filtering policies, every endpoint is shielded from internet-based threats at the DNS level—before they can do any harm.	Fewer security incidents, less downtime, and a reduced burden on internal IT resources. It also helps enforce acceptable use policies by preventing access to non-work-related or high-risk content, which can improve productivity and support compliance with industry regulations.
Security Operations Centre (SOC) for M365 tenant	External network security monitoring resource, facilitated by SOC agents that is deployed across your M365 tenant	Continuously monitors your M365 tenant for threats like phishing, malware, suspicious sign-ins, and unauthorised data access. It uses Microsoft tools like Defender for Office 365, Defender for Endpoint, and Sentinel to detect and investigate security alerts across email, identity, and devices in real time. Once threats are identified, the SOC takes action to contain and remediate incidents quickly. The SOC also tunes alert rules, analyses threat patterns, and refines policies to strengthen your tenant's overall security posture, ensuring resilient defense across all M365 services.	Faster detection and response to threats targeting your M365 environment, reducing the risk of data breaches and service disruptions. It enhances visibility across email, identity, and device activity, allowing for proactive defense and continuous improvement of security posture. Ultimately, it helps maintain trust, compliance, and operational continuity by keeping your M365 tenant secure and resilient.

efex
SMARTER TECH FOR AMBITIOUS BUSINESS

Managed Cyber

Next level protection & IT support for every business

Inclusion	What is it?	What does it do?	The outcome you can expect
Security Operations Centre (SOC) for endpoints & servers	External network security monitoring resource, facilitated by SOC agents that are deployed to all endpoints	Provides continuous, behind-the-scenes protection for endpoints and servers by monitoring for suspicious activity, system anomalies, and potential threats in real time. Whether it's a workstation or server - every log event, system change, and user action is quietly analysed and correlated against known threat patterns. efex's SOC agent collects critical telemetry such as failed login attempts, unauthorised service changes, and unusual network behaviour, then securely transmits this data to a centralised monitoring platform. There, a team of expert analysts investigate alerts, hunt for hidden threats, and responds to incidents before they escalate. This proactive monitoring ensures even the most subtle signs of compromise are detected early, helping prevent breaches and minimise damage. For the endpoint, it's like having a 24/7 cybersecurity expert watching over it - ready to act the moment something suspicious occurs.	Stronger protection against cyber threats, reduced complexity and cost. It also supports compliance with industry regulations, ensuring security logs are collected, analysed, and retained properly.
Advanced Security Operations Centre (SOC) / Security Information & Event Management (SIEM)	External network security monitoring resource, facilitated by SOC agents deployed to all endpoints, servers, network devices	By collecting and correlating data from endpoints, servers, network devices, and cloud services, efex's SIEM platform enables security teams to identify suspicious activity in real time. The Advanced SOC enhances this capability with expert monitoring, AI-driven analytics, and automated workflows that streamline threat hunting and ensure compliance with industry regulations. and cloud services.	A stronger security posture, reduced risk of breaches, and improved operational resilience. The system accelerates response times while also enabling forensic investigations and audit readiness through detailed logging and reporting to help meet compliance requirements.
Advanced conditional access	Security management tool	Enforces access policies using real-time context—such as user identity, device health, location, and risk level—to ensure only trusted users on compliant devices in secure locations can access sensitive resources. This adaptive, seamless approach bolsters identity protection, reduces threat exposure in hybrid and remote environments, and helps prevent unauthorised access without disrupting the user experience.	Enhanced data protection, reduced risk of credential compromise and improved compliance with security standards. Granular control over who can access what, when, and how—enabling secure collaboration without sacrificing productivity.
Application whitelisting	Security management tool	Provides a powerful layer of endpoint protection ensuring only explicitly approved applications can run on a device—everything else is automatically blocked. From the user's perspective, their computer or server is safeguarded against unauthorised software, including malware, ransomware, and unapproved tools, without them needing to take any action. When efex first enables this service, the system enters a "learning mode" to catalog all legitimate applications currently in use. Once the environment is understood, efex locks down the system so that only those known, trusted applications can execute. If a user needs to install new software, they can simply request approval, which can be granted quickly—often within minutes—without compromising security. This approach not only prevents cyber threats from executing but also eliminates the risk of unauthorised applications, ensuring a consistent and secure application environment across all endpoints. For users, it's a seamless experience that keeps them productive while efex silently enforces strict security controls in the background.	A dramatic reduction in the risk of malware, ransomware and unauthorised software execution because only pre-approved trusted applications can run on company devices.
Copilot & advanced workflow support	Digital enablement resource	Boosts productivity by streamlining automation and providing intelligent assistance across business operations. It helps users create content, analyze data, and manage tasks efficiently. With advanced workflow support, it minimizes manual effort and errors, enabling teams to focus on strategic work while enhancing consistency, speed, and agility.	Intuitive guidance and automation via Microsoft Copilot that adapts to the roles and tasks of users, which in turn reduces friction and boosts productivity.
Incident response & problem management	Technology management platform	Provides a structured and proactive approach to identifying, managing, and resolving IT incidents and underlying problems. With real-time monitoring, automated alerts, and guided workflows, efex ensures incidents are swiftly contained and resolved to minimise disruption. The platform goes beyond reactive fixes by analysing root causes, tracking recurring issues, and implementing long-term solutions that prevent future incidents. This dual-layered approach maintains service continuity while continuously improving system reliability.	Faster recovery times, reduced downtime, and improved user satisfaction. The system promotes transparency and accountability through detailed incident tracking, reporting, and communication tools. Over time, this leads to a more resilient IT environment, lower operational costs, and a culture of continuous improvement.
Essential 8 gap analysis assessment & report	Strategic cyber security review	Evaluates your organisation's alignment with the Australian Cyber Security Centre's (ACSC) Essential Eight mitigation strategies. Through a detailed assessment, efex identifies gaps in your current security posture across key areas such as application control, patch management, user access, and system hardening. The process includes reviewing existing controls, assessing maturity levels, and providing actionable recommendations to help you strengthen defenses and meet compliance requirements.	Gain a clear understanding of your cybersecurity strengths and vulnerabilities, along with a prioritised roadmap that guides remediation efforts, improves risk management, and supports alignment with government and industry standards.
Digital footprint monitoring	Security management tool	Continuously assesses how a business appears from the outside—just like a hacker would see it. efex is constantly scanning the internet for exposed assets, misconfigured systems, outdated software, and other vulnerabilities tied to the domain, IP addresses, and public-facing infrastructure. If a device or service is unintentionally exposed or behaving in a way that could attract cyber threats, efex detects it and alerts the business before it becomes a target. This proactive monitoring ensures users aren't unknowingly operating in a risky environment and their systems aren't contributing to the business's external risk profile. It's a silent but powerful layer of defense, ensuring the digital presence for every user is secure, compliant, and protected against attacks.	Stronger security, enhanced compliance, and greater confidence in your digital presence while effectively protecting your reputation, data, and operations.
Quarterly penetration testing	Security simulation software	Simulates real-world cyberattacks to uncover vulnerabilities across your digital infrastructure. By emulating the tactics of malicious actors, efex identifies weaknesses in networks, systems, and applications before they can be exploited. The testing process includes comprehensive analysis and reporting, giving your team clear visibility into potential risks and actionable recommendations for remediation. This hands-on approach ensures your organisation is prepared, resilient, and continuously improving its security posture.	Enhanced threat awareness, reduced risk of data breaches, and strengthened compliance with industry standards. Gain confidence in your ability to detect and defend against cyber threats, supported by expert insights and targeted mitigation strategies.
Phishing simulations	Security simulation software	Immerses users in realistic, evolving cyberattack scenarios designed to sharpen their instincts and improve their ability to spot malicious emails. Without knowing they're part of a training exercise, users receive simulated phishing messages that closely mimic real-world tactics like fake invoices, urgent password reset requests, or impersonated executives. These simulations test users' reactions in a safe environment, helping them learn to pause, question, and verify before clicking. If a user interacts with a simulated threat, they're immediately guided through a brief, targeted training module that explains what they missed and how to avoid similar traps in the future. Over time, this builds stronger awareness and resilience, turning everyday users into active participants in the company's cybersecurity defense. It's a practical, hands-on learning experience empowering users to recognise and resist real phishing attempts with confidence.	Fewer successful phishing attempts, and reduced risk of data breaches thanks to employees that are more cyber-aware. The business now maintains a stronger cybersecurity posture. It also demonstrates a proactive commitment to cybersecurity, which can support compliance with industry regulations and build trust with clients and partners.

efex
SMARTER TECH FOR AMBITIOUS BUSINESS

Managed Cyber

Next level protection & IT support for every business

Inclusion	What is it?	What does it do?	The outcome you can expect
Monthly cyber reporting	Technology documentation	efex's monthly technology reporting provides clear, actionable insights into your IT environment, helping you stay informed, proactive, and in control. Each month, efex delivers a comprehensive report that covers system performance, security events, service usage, support activity, and compliance status. These reports are designed to translate technical data into business-relevant insights, enabling stakeholders to make informed decisions, track progress against strategic goals, and identify areas for improvement. With visual summaries and expert commentary, efex ensures your technology landscape is transparent and aligned with your business objectives.	Improved visibility, better risk management, and stronger alignment between IT and business strategy. By regularly reviewing trends and performance metrics, you can anticipate issues before they escalate, optimise resource allocation, and demonstrate accountability to leadership and auditors, empowering you to make smarter, data-driven decisions that support growth, security, and operational excellence.
Technology roadmapping	Technology strategy development & planning	A strategic service that aligns your IT investment with long-term business goals. Through collaborative planning and expert analysis, efex works with you by identifying priorities and setting timelines to develop a clear, forward-looking roadmap that outlines key technology initiatives, upgrade cycles, risk mitigation strategies, and innovation opportunities. This roadmap is tailored to your unique environment and growth objectives, ensuring your technology evolves in step with your business and empowers you to make informed, future-ready decisions. With regular reviews and updates, your roadmap remains agile and responsive to change.	Greater clarity, reduced risk, and more efficient use of IT resources. A structured plan supports budgeting, minimises reactive spending and ensures technology remains an enabler—not a barrier—to success.
Phishing resistant / FIDO2 compliant Multifactor authentication	Passwordless security software	Protects user identities with strong, phishing-resistant authentication. By leveraging public key cryptography and hardware-backed credentials, efex ensures that access to systems and data is granted only to verified users through secure devices. This approach eliminates reliance on traditional passwords, reducing the risk of credential theft and improving user experience. efex's MFA integrates seamlessly with existing infrastructure and supports a wide range of devices and platforms, making it ideal for organizations seeking scalable, future-ready identity protection.	Significantly enhanced security, reduced attack surface, and simplified access management. Users benefit from faster, more secure logins without the burden of remembering complex passwords, while IT teams gain confidence in the integrity of authentication processes. Also supports compliance with cybersecurity standards and helps defend against increasingly sophisticated threats.
Microsoft 365 hardening	Security configuration tool	Applies security best practices to protect your organisation's data, users, and devices. It includes enforcing multifactor authentication, securing endpoints with antivirus and anti-phishing tools, blocking malicious links and attachments, and applying consistent app and device configurations. It also enables remote wipe, conditional access, and compliance monitoring to ensure only trusted users and devices can connect to company resources	Creates a safer, more consistent work environment with secure access and fewer disruptions from cyber threats.
Advanced vulnerability scanning	Security management tool	Identifies and prioritises security weaknesses across endpoints, cloud apps, identities, and containers. It uses agentless scanning, threat intelligence, and contextual risk analysis to uncover vulnerabilities and misconfigurations.	Fewer disruptions, safer devices, and better awareness of threats for all users.