Maximize the Value of Your Microsoft Security Investment and Unlock Your Security Potential

CRITICALSTART®

Introduction

If you've been thinking about upgrading your organization's security from Microsoft 365 E3 to E5, or maybe your organization has already upgraded for non-security reasons and you're trying to decide if E5 is for you, there's never been a better time to make the leap.

Some IT decision-makers have been holding off, worried about cost or deployment complexities. Others are interested in the advanced threat protection capabilities of E5 and the potential for tool consolidation and simplification across vendors but are concerned with the expertise required to operationalize the advanced capabilities. Don't be! With Managed Extended Detection and Response (**MXDR**) services and Microsoft expertise from CRITICAL**START**®, transitioning to E5—and getting the most out of your Microsoft Security investment—can be a reality.

Microsoft E5 Offers Bold New Security Tools

Many organizations adopt Microsoft E5 to secure their infrastructure with the advanced capabilities delivered by Microsoft 365 Defender. By that logic, upgrading to E5 is a no-brainer—it has a greatly expanded new suite of Defender security tools compared to E3.

Advanced Threat Protection is one of the primary differences between E3 and E5 licenses. E5 licenses come with Advanced Threat Protection (**ATP**), a set of advanced security features designed to protect against sophisticated cyber threats such as phishing, malware, and ransomware attacks. This feature provides an additional layer of security to protect sensitive data and systems.

E5 licenses also include Microsoft Defender for Cloud Apps, which offers visibility and control over cloud applications and services. Administrators can monitor user activity and data usage across cloud services, identify potential security risks, and take appropriate action to protect sensitive data.

Identity and Access Management (**IAM**) features, such as multi-factor authentication and conditional access, are included in both E3 and E5 licenses. However, E5 licenses have more advanced IAM capabilities, such as Privileged Identity Management and Microsoft Entra ID Premium P2. These features give administrators greater control over sensitive data and systems access.

As you can see, upgrading to E5 licenses has many benefits that can help you overcome security risks, including reducing the number of siloed security tools, improving data analytics, and adding advanced threat capabilities to eliminate coverage gaps.

With E5 licenses, you can streamline your security operations by consolidating multiple security tools into one unified platform, making managing and monitoring security risks easier. This can also reduce the costs associated with maintaining multiple security tools.

E5 licenses also provide advanced data analytics capabilities, allowing you to identify and respond to security threats quickly in real time. With the ability to promptly analyze security data, you can take immediate action to prevent or mitigate security breaches.

Another benefit of E5 licenses is advanced threat capabilities. With features such as ATP and Microsoft Defender for Cloud Apps, you can protect against sophisticated cyber threats like phishing, malware, and ransomware attacks. These features offer an additional layer of security to protect your sensitive data and systems.

E5 licenses also offer cross-domain threat detection capabilities, allowing you to monitor and protect your entire network, including on-premises and cloud environments, giving you a comprehensive view of your security posture and making it easier to identify and address potential security risks.

Microsoft 365 Defender

- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Entra Identity Protection
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for Servers

Overcoming the Barriers to Better Security Outcomes

Thinking of upgrading from E3 to E5 security licenses but worried about the added costs, complexity, and compatibility issues? No worries, we've got you covered!

Customers looking to upgrade to an E5 license to take advantage of the advanced security capabilities critical in protecting against cyber threats can find support from the MXDR and Critical Start Services. With our expert guidance, you can overcome the complexity and compatibility issues associated with upgrading to E5 licenses and reduce your total cost of ownership by streamlining security operations while improving the speed of detection and response against threats. Our team works closely with you to run a detailed value calculator and replacement assessment to evaluate what to replace.

First, our focus is on planning and implementing the solutions that provide the best outcomes to achieve your business objectives and protect what's most important. Our Dedicated Microsoft Services team brings a Quick Start solution approach to identify the most critical to monitor, gain visibility into, and protect and respond to.

Then, to actualize cost optimization of your E5 license, Critical Start remains committed to delivering the outcomes that simplify the complex, reduce operational costs, and achieve higher Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) outcomes. Our dedication to delivering the best Managed Detection and Response (**MDR**) services and our top-notch Professional Services capabilities can help you achieve your security goals at a pace you feel comfortable with while protecting what matters.

By partnering with Critical Start and Microsoft, you will effectively identify and prioritize security risks, improve your security posture, and reduce the risk of breach with the security features included in your E5 license.

Microsoft Security Expertise with Professional Services

Given the volume and complexity of identities, data, applications, devices, and infrastructure, it is essential to learn how secure your organization is right now and how to mitigate and protect against threats moving forward. That is why Critical Start, along with our Partners, provides Microsoft Security Professional Services, offering workshops, assessments, and deployment services to help you explore, optimize, and improve your security posture.

Overcoming the Barriers to Better Security Outcomes (continued)

Microsoft Workshops

Workshops provide hands-on experiences designed to help you maximize existing Microsoft security infrastructure while learning how to put next-generation Microsoft security tools to work for you. These include:

SIEM + XDR Workshop	Learn how Microsoft Sentinel and Microsoft 365 Defender can help your organization use intelligent security analytics and threat intelligence to detect and quickly stop active threats.
Endpoint Management Workshop	Learn the power of modern device management and how to leverage intelligent security, risk-based controls, zero-touch provisioning, advanced analytics, and deep integration to build management policies that protect your users, company data and devices.
Secure Identities & Access Workshop	Learn how to ensure the right people are accessing the right information, securely. In this workshop, you will learn how identity is the fundamental pillar of an integrated security philosophy and end-to-end security strategy.

Security Assessments

The Critical Start Microsoft Professional Services assessments thoroughly analyze your Microsoft environment to capture your current configuration state and provide detailed recommendations to improve overall security posture.

Microsoft 365 Defender Security Assessment	This assessment addresses misconfigurations and poor adoption practices by comparing current configurations to Microsoft and industry best practices. Critical Start conducts a thorough end-to-end analysis of your environment to address these challenges.
Microsoft Sentinel Security Assessment	This assessment is designed to evaluate your Microsoft Sentinel environment to ensure best practices are being followed. This not only looks for misconfiguration but also opportunities for optimization to reduce ingest cost, develop stronger detections, and identify unused features to optimize your investment.

Unlocking the Power of Microsoft E5

Here's how to make them even better.

There's no denying that Microsoft Security is moving to stay ahead of constantly evolving security threats—the expansion of the Defender suite in Microsoft 365 E5 is proof positive of that. So are the awards and recognition the products within the suite have received, like being included as a leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms and five other Gartner Magic Quadrant reports.[1]

But with the hyper-complexity of today's security environment, compounded by a shortage of cybersecurity talent, an aggressive and proactive approach to cybersecurity becomes critically important. With an attack surface that is constantly changing, where access roles are dynamic and devices and applications request and keep more data, tools alone are not enough.

Tools, talent, and new processes and methodologies are needed for crossenterprise visibility into threat detection, investigation, and response. Microsoft has made great strides in this area, with a suite of products to not only identify a threat as it happens but to deliver visibility as the threat attempts to move across an organization's security landscape.

Still, while Microsoft E5 provides a robust set of advanced security tools, even the best email security engineers and analysts might become overwhelmed with alert volume and complexity of event correlation. We can help you make the most effective use of this information and maximize the potential of these technologies.

What's needed is a team with expertise and know-how to make sense of Microsoft's cross-enterprise threat detection and investigation capabilities. With the right mix of technology, talent, and process in place, it becomes possible to radically reduce alerts and actively respond to threats.

[1]*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021*

Maximize the Value of Microsoft E5 Security with MXDR

Managed Detection & Response Solutions and Services from Critical Start

Operationalize Microsoft 365 Defender for complete threat detection and response outcomes

It's no longer enough to monitor only endpoints. Cyberattacks are increasing across multiple vectors, including compromised credentials, email phishing, and 3rd party cloud applications.

But where do you start? Organizations need a solution that can help them move to or optimize the power of their Microsoft Security investment for protection beyond the endpoint.

Expert Guidance on Best Practices:

Receive invaluable advice on implementing and managing your Microsoft Security solutions, ensuring you're optimized and protected against ever-evolving cyber threats.

Seamless Integration with Existing Infrastructure:

Benefit from smooth integration of Endpoint Detection & Response (EDR), SIEM, and XDR capabilities into your existing security infrastructure for a cohesive and efficient security ecosystem.

Optimized Configuration and Tuning:

Get expert assistance in fine-tuning and optimizing the configuration of your Microsoft Security solutions, ensuring maximum effectiveness and protection.

Detect and disrupt attacks during the attack chain with our expert MXDR guidance and support.

Speed up investigation and response across Microsoft Security environments with an extended team of security experts.

> We have a small security team and were using disparate security controls that didn't work well together – it was not an effective strategy. Our company was all-in on Microsoft E5, but we weren't using the complete Defender security suite. It was a simple path forward to bring integrated threat protection from Critical Start MXDR services for Microsoft services together to drive simplified, better security outcomes and improve our ability to meet global compliance requirements.
>
> - Security Manager Microsoft Sentinel, Microsoft Defender for Endpoint, Microsoft 365 Defender user

Tools Backed By Expertise Are More Effective

Given the volume and complexities of identities, data, applications, devices, and infrastructure, developing a strategic plan for your organization's priorities is essential.
Our Microsoft Security experts help you determine how secure your organization is now and how to mitigate and protect against threats moving forward. Our managed services are focused on applying Microsoft security best practices and highfidelity threat detection, with continuous tuning as new risks are identified.

The Critical Start Approach

Protect Everything Everywhere

- Develop a strategic Professional Services-led plan customized for your organization's priorities
- Focus on implementation and onboarding to apply Microsoft security best practices and high-fidelity threat detection
- Continuously fine-tune as new risks are identified
- Apply comprehensive coverage against attacks targeting your organization with the most effective MXDR services powered by the industry's only **Cyber Operations Risk and Response™ platform**

Drive actionable insights from your Microsoft Security Solutions with expert guidance, Microsoft best practices and support.	Extend your team with complete 24x7x365 detection, investigation, and response.	Measure your current security operations, pinpoint opprtunities for improvement, and bolster your defenses.	Minimize the impact of a breach and get peace of mind with IR experts.
MICROSOFT SECURITY CONSULTING	MANAGED DETECTION & RESPONSE SERVICES	MICROSOFT SECURITY CONSULTING	INCIDENT RESPONSE SERVICES

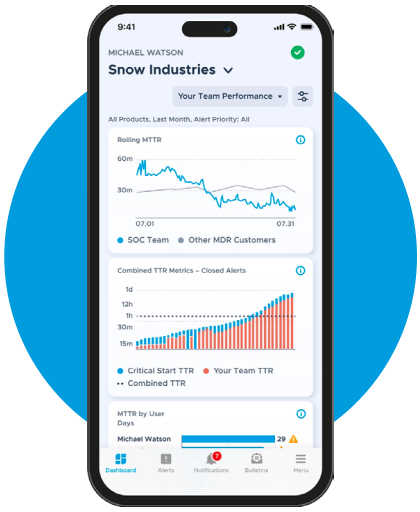
The Critical Start Approach

Extend your Capabilities to Quickly Detect and Respond to Threats

When minutes count, our Microsoft security experts can become an extension of your team and provide remediation and response actions to the threat as soon as it's detected. You'll get:

- Configuration and optimization of your Microsoft Security tools and our platform to eliminate false positives (>99% of alerts) and dramatically reduce alert overload
- Cross-domain threat protection for use cases like email phishing, brute force and stolen credential attacks and attacks against cloud apps
- Monitoring, investigation, and resolution of all alerts (**EDR, XDR, and SIEM**) — 24x7x365 with 60-minute or less Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) service level agreements (**SLAs**)
- Operationalized Threat Intelligence that increases your effectiveness to detect attacks
- NIST CSF maturity and **MITRE ATT&CK® Framework** coverage reporting
- Full visibility and response actions via our platform and full-parity MOBILE**SOC®** application

Our platform delivers risk reduction and operational metrics focused on continuous improvement.



MOBILESOC, an iOS and Android application, let's you contain breaches right from your phone.

The Critical Start Approach

Advance security maturity with a focus on continuous improvement and risk reduction

With Critical Start, you have access to end-to-end solutions and services that move with you on your Microsoft security journey, helping anticipate risk and strengthening security posture. What sets us apart:

- **Microsoft expertise** - Our Microsoft security experts help you determine how secure your organization is now and how to mitigate and protect against threats moving forward.
- **Workshops and professional services** - Designed to help you reduce security tool complexity while optimizing deployment and configuration of your Microsoft E5 investment for the best breach prevention per dollar spent.
- **Threat protection and risk reduction platform** - Our platform enables the Critical Start Risk and Security Operations Center (**RSOC**) to become a true extension of your security team, working together in real-time, 24x7x365.

Positive Outcomes You Can Rely On

Consolidate visibility and coverage across all attack vectors

The better you know your security controls, the greater your ability to minimize risks. Microsoft Security experts from Critical Start can operationalize your security controls with Microsoft Security Best Practices. Our integrated MXDR services for Microsoft give you unmatched visibility across your Microsoft ecosystem to detect and respond to every threat at scale.

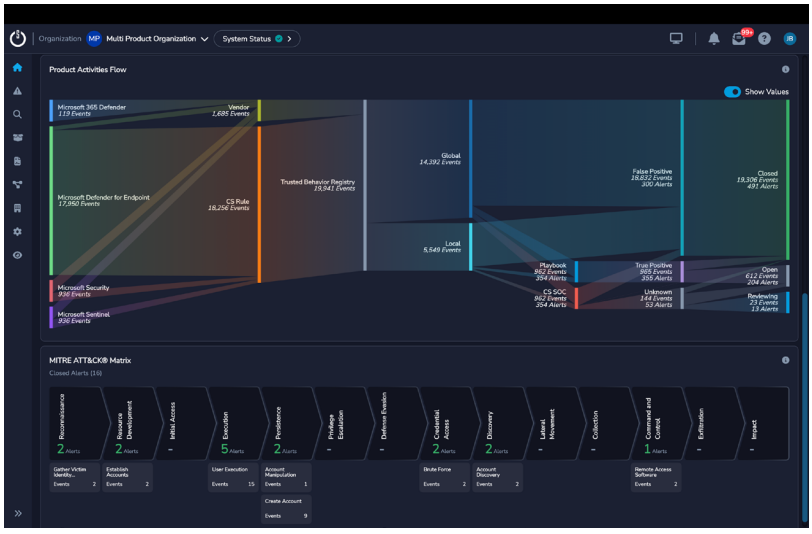
Disrupt the cross-domain attack chain

Highly scalable detection capabilities utilizing automation, event correlation, and proven threat investigation methodologies reduce risk and prevent attacks. MXDR services for Microsoft extend your security defenses across your domains—from endpoint to email, user credentials, and cloud apps. Our platform monitors every single activity while our experts provide the tuning recommendations you need to protect your organization from security threats while minimizing risk..

Real-time risk and operational metrics

Our team of Microsoft security experts leverages our integration with Microsoft Security to detect, investigate, and respond with the right actions before threats can disrupt your business. Our outcome-based approach focuses on delivering value across areas critical to your organization.

- **Situational awareness**: By delivering actionable views of attacks in progress with clear, step-by-step response guidance, security teams gain situational awareness they can use.
- **Team efficiency:** Measuring the MTTR for analysts and teams drives continuous improvement, productivity, and team efficiency.
- **Effectiveness**: Critical Start MDR maps detection content to the MITRE ATT&CK Framework, enabling risk-based decision-making and improving attack coverage effectiveness.
- **Investment guidance**: We deliver data and reporting that articulate the value of our MDR service to help you align cybersecurity investments with business outcomes.



A dashboard showing risk and operational metrics, including a history of alert investigations and response activity.

> Our existing security strategy was not effective, with disparate security controls that didn't function well together to meet global compliance requirements. As a small security team, we knew we could do better. Bringing together the Microsoft E5 security suite with the Critical Start MXDR services for Microsoft has decreased our overall security spend, allowed my team to focus on higher-priority business initiatives, and has driven better security outcomes.
>
> - Security Manager Oil & Energy Microsoft Sentinel, Microsoft Defender for Endpoint, Microsoft 365 Defender user

For more information, contact us at:
https://www.criticalstart.com/contact/