

## Microsoft Security Migrations

Migrate with confidence to the Microsoft Security ecosystem.

*As security priorities evolve, many organizations are rethinking the tools in their environment. The Microsoft Security ecosystem offers a unified, cloud-native alternative to simplify operations and improve integration.*

### Making the shift to Microsoft Security

The threat landscape continues to shift – faster, more complex, and increasingly cloud-driven. As organizations modernize their security posture, many are evaluating migrations to integrated solutions within the Microsoft Security ecosystem. Microsoft offers a unified, cloud-native approach to threat detection, response, and identity protection – aligned with the needs of today’s hybrid enterprise.

LevelBlue offers three key services to support your migration to Microsoft Security:

- **Microsoft Sentinel:** Modernizing SIEM with Sentinel
- **Microsoft Defender XDR:** Consolidating detection and response through Defender XDR
- **Microsoft Entra ID:** Strengthening identity foundations with Entra ID

These solutions are designed to work together, offering a more connected approach to monitoring, investigation, and access control across hybrid environments. Our migration services help clients move with confidence – enhancing value while minimizing disruption.

### Migration to Microsoft Sentinel

LevelBlue adopts a four-phased approach for your migration to Microsoft Sentinel:

- 1 **Discovery and Assessment:** Assess your existing SIEM environment to understand architecture, data sources, log volumes, use cases, and analytic rules, and develop a tailored migration strategy.
- 2 **Configuration and Build:** Design and deploy the Sentinel architecture, including workspace setup, data connectors, and access controls.
- 3 **Validation and Testing:** Review data ingestion and validate parsing, field mappings, rule logic and alerting, and dashboard/report outputs.
- 4 **Optimization and Operational Handoff:** Refine configurations and provide training, documentation, and knowledge transfer to enable effective Sentinel operations.

### Benefits

- Access a team of LevelBlue consultants with deep subject matter expertise in Microsoft Security.
- Unlock the value of Microsoft Security.
- Accelerate time to value by quickly enabling Microsoft Security capabilities with expert-led setup.
- Reduce risk of misconfiguration, downtime, or security gaps during the migration process.
- Optimize configurations and integrations to fit your specific environment and security needs.
- Align your security approach with best practices and future initiatives during the transition.
- Enable operational readiness through tailored training, documentation, and support.

## Migration to Microsoft Defender XDR

LevelBlue adopts a four-phased approach for your migration to Microsoft Defender XDR:

- 1 Discovery and Assessment:** Evaluate your current security ecosystem, including EDR, email, identity, and endpoint protections, to identify existing capabilities, integration points, and migration requirements.
- 2 Solution Design and Configuration:** Develop a tailored Defender XDR architecture, configure Defender components, and define policies based on organizational risk and operational needs.
- 3 Validation and Testing:** Validate data ingestion, alerting, and automated response across workloads.
- 4 Optimization and Operational Handoff:** Fine-tune configurations and provide knowledge transfer, training, and tuning support for ongoing monitoring, threat response, and policy adjustments.

## Migration to Microsoft Entra ID

LevelBlue adopts a five-phased approach for your migration to Microsoft Entra ID:

- 1 Discovery and Assessment:** Evaluate your current identify infrastructure, authentication methods, and application dependencies to shape a tailored migration plan.
- 2 Platform Configuration and Integration:** Configure Entra ID tenants and domains, set up conditional access and security policies, and integrate authentication methods (e.g., passwordless, FIDO2).
- 3 Application Migration:** Prioritize application migration, update application configurations, validate authentication/ authorization flows, and coordinate testing with application owners.
- 4 User Migration and Testing:** Conduct controlled user migrations, validate user attributes and session behavior, monitor sync processes, and address exceptions and policy conflicts.
- 5 Optimization and Operational Handoff:** Fine-tune configurations, provide documentation and training, and transition operations to your internal team or support model.

## Microsoft Credentials and Certifications

LevelBlue is endorsed and validated by Microsoft as a leading cybersecurity partner:

### Certified Microsoft AI Cloud Solutions Partner:

- Microsoft Advanced Security Specializations: Cloud Security, Threat Protection, and Infrastructure Azure
- Microsoft Intelligent Security Association (MISA) Member
- Microsoft Verified MXDR Partner
- Participation in Cybersecurity Investment (CSI) and FastTrack Ready Programs

### Microsoft Certified Experts:

- Microsoft MVP 'Most Valuable Professional' (Azure Security)
- Azure Security Architect Expert
- Azure Administrator
- Azure Security Engineer



### Longstanding Microsoft Recognition

LevelBlue has been recognized by Microsoft over the years:

- Microsoft 'Top Managed SOC' (1st Place)
- Microsoft Threat Indicator Top Contributor (1st Place)
- Top GitHub Contributor