Trustwave®

Microsoft Security Migrations

MIGRATE WITH CONFIDENCE TO THE MICROSOFT SECURITY ECOSYSTEM

Benefits

- Access a team of Trustwave consultants with deep subject mater 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.

As security priorities evolve, many organizations are rethinking the mix of tools in their environment. Whether due to cost, complexity, or a shift in strategic direction, migrating from existing platforms is becoming increasingly common. The Microsoft Security ecosystem – spanning Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Entra ID – offers a unified, cloud-native alternative that aligns well with today’s business and technical needs.

These migrations are not just about replacing tools – they are about simplifying operations, improving integration, and gaining better long-term value from your Microsoft investments. With a thoughtful, phased approach, organizations can make the transition with minimal disruption while setting themselves up for greater efficiency and visibility moving forward.

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

1. Migration to Microsoft Sentinel
2. Migration to Microsoft Defender XDR
3. Migration to Microsoft Entra ID

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.

Organizations can prioritize three core areas when making the shift:

- **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

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

1. **Discovery & 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 & Build:** Design and deploy the Sentinel architecture, including workspace setup, data connectors, and access controls.
3. **Validation & Testing:** Review data ingestion and validate parsing, field mappings, rule logic and alerting, and dashboard/report outputs.
4. **Optimization & Operational Handoff:** Refine configurations and provide training, documentation, and knowledge transfer to enable effective Sentinel operations.

Migration to Microsoft Defender XDR

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

1 **Discovery & 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 & Configuration:** Develop a tailored Defender XDR architecture, configure Defender components, and define policies based on organizational risk and operational needs.

3 **Validation & Testing:** Validate data ingestion, alerting, and automated response across workloads.

4 **Optimization & 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

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

1 **Discovery & Assessment:** Evaluate your current identify infrastructure, authentication methods, and application dependencies to shape a tailored migration plan.

2 **Platform Configuration & 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 & Testing:** Conduct controlled user migrations, validate user attributes and session behavior, monitor sync processes, and address exceptions and policy conflicts.

5 **Optimization & Operational Handoff:** Fine-tune configurations, provide documentation and training, and transition operations to your internal team or support model.

Microsoft Credentials & Certifications

Trustwave 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

Member of
Microsoft Intelligent Security Association
Microsoft Verified Managed XDR Solution
Microsoft Solutions Partner
Security
Cloud Security
Threat Protection
Infrastructure Azure
Microsoft FastTrack Partner
Microsoft MVP 2023 Most Valuable Professional
Microsoft Certified Cybersecurity Architect Expert
Microsoft Certified Azure Administrator Associate
Microsoft Certified Azure Security Engineer Associate

Longstanding Microsoft Recognition

Trustwave has been recognized by Microsoft over the years:

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

About Trustwave

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats.

Trustwave's comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes its client's cyber investment, and improves security resilience. Trusted by thousands of organizations worldwide, Trustwave leverages its world-class team of security consultants, threat hunters, and researchers, and its market-leading security operations platform to decrease the likelihood of attacks and minimize potential impact.

Trustwave is an analyst-recognized leader in managed detection and response (MDR), managed security services (MSS), cyber advisory, penetration testing, database security, and email security. The elite Trustwave SpiderLabs team provides industry-defining threat research, intelligence, and threat hunting, all of which are infused into Trustwave services and products to fortify cyber resilience in the age of inevitable cyber-attacks.

www.trustwave.com