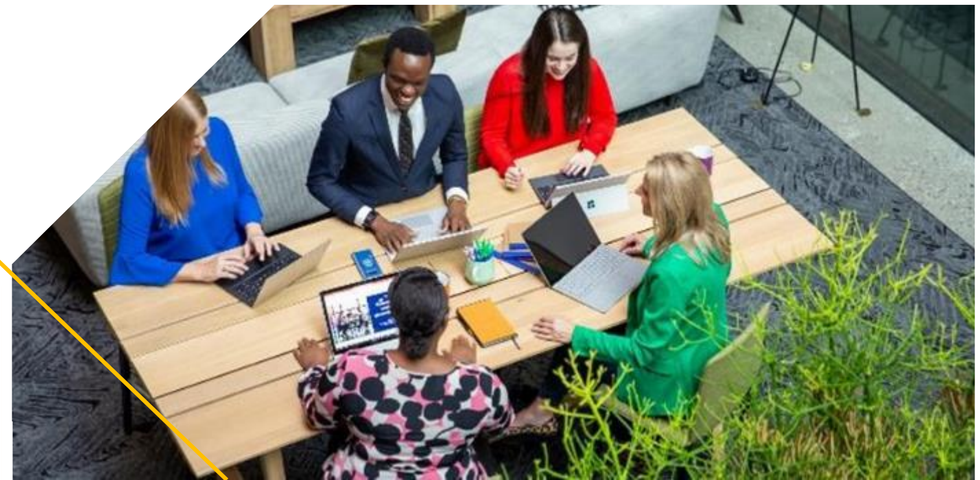
BONELLI SYSTEMS

Microsoft Solutions Partner
Data & AI Azure
Digital & App Innovation Azure
Infrastructure Azure
Security

Security Operations & XDR

Defender XDR, Sentinel SIEM, SOAR, and SOC Operationalization

2025



Cybersecurity threats demand integrated detection and response

Organizations face sophisticated threats across multiple attack vectors. Siloed security tools, alert fatigue, ransomware threats, and compliance mandates require integrated visibility, automation, and proven recovery capabilities.

Primary challenges

Siloed security tools create visibility gaps across endpoints, identities, email, and cloud apps. Security teams cannot correlate alerts across attack vectors, missing coordinated threats.

Ideal solution

Alert fatigue overwhelms SOC teams. Without SOAR automation, analysts spend excessive time investigating false positives and manual tasks instead of hunting threats. Burnout increases.

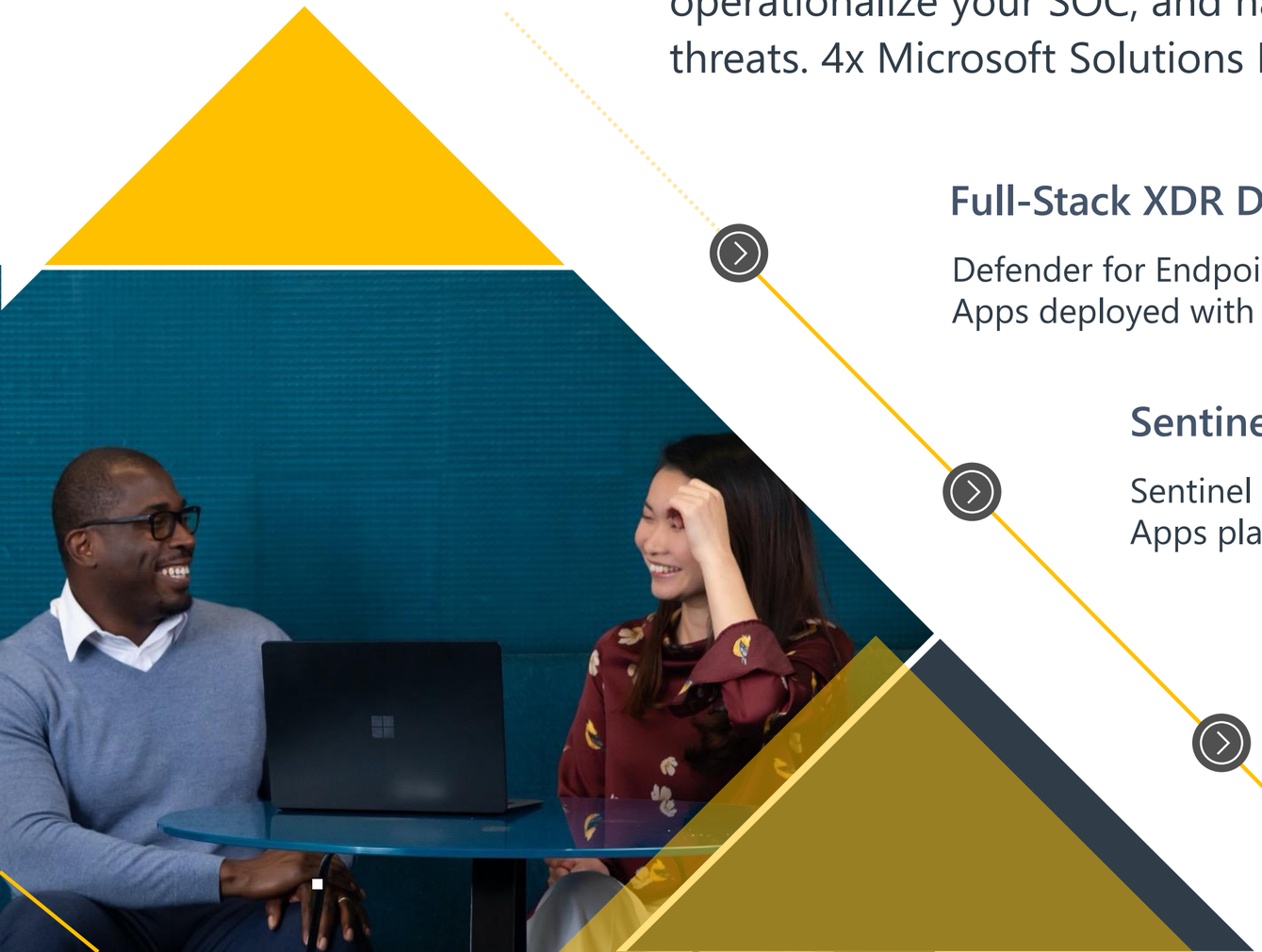
Desired outcomes

Ransomware threats require both prevention and proven recovery. Organizations need secure environments they can stand up rapidly if the worst happens. Business continuity depends on it.

BONELLI SYSTEMS

Security Operations Platform

We deploy complete Microsoft Defender XDR and Sentinel stacks, operationalize your SOC, and harden your environment against modern threats. 4x Microsoft Solutions Partner.



Full-Stack XDR Deployment

Defender for Endpoint, Identity, Office 365, and Cloud Apps deployed with custom detection rules and.

Sentinel SIEM with SOAR

Sentinel deployment with custom analytics rules, Logic Apps playbooks for automated investigation,

Environment Hardening & Resilience

CIS Benchmark enforcement across endpoints, servers, M365, and Azure.

Bonelli Systems, Security Operations Platform, and Microsoft Defender XDR

Together we deliver unified security that eliminates tool sprawl. Our Defender XDR integration with Sentinel provides single-pane-of-glass visibility across all attack vectors. We maximize ROI on Microsoft 365 E5 licensing by activating all security features with proper tuning.

Azure-Native Security Architecture

Security infrastructure runs on Azure with Azure Firewall, Private Endpoints, and NSGs providing defense-in-depth for all workloads.

E5 Security Optimization

Maximize ROI on Microsoft 365 E5 licensing by activating all security features with proper tuning and ongoing SOC-ready management.

XDR + Sentinel Integration

Full Defender XDR integrated with Sentinel for unified SIEM/SOAR. Single-pane-of-glass visibility across all attack vectors with automated threat.

Customer success: Enterprise client deploys unified security operations

Client engaged to deploy full Defender XDR suite across enterprise with device tagging and attack surface reduction. Sentinel was onboarded with M365, Entra ID, Azure, and firewall logs. Custom analytics rules and incident taxonomy were tuned. SOAR playbooks built in Logic Apps for auto-isolation and user suspension.

Enterprise XDR Deployment

Full Defender XDR deployed across enterprise with custom detection tuning, Application Control, and Device Control policies.

SOAR Automation

Logic Apps SOAR playbooks for automated containment: auto-isolation, user suspension, IOC enrichment for rapid incident response.

Purple-Team Validation

Purple-team exercises validated detection coverage. Hunting queries, watchlists, and workbook dashboards operationalized for SecOps.

Channel Partner success: Enterprise builds resilient airgapped environment

Enterprise client engaged to proactively build tertiary airgapped environment to safeguard against ransomware threats. 50+ servers were built from the ground up across 20+ fully segmented virtual networks, with complete Defender XDR and Sentinel stack deployed, and 100TB of database data migrated to Azure SQL Managed Instances.

Airgapped Infrastructure

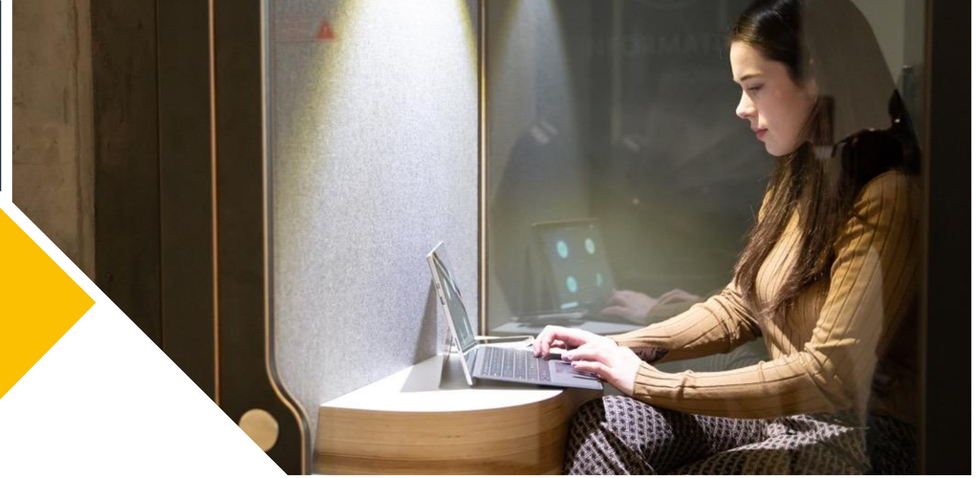
50+ servers built from ground up in airgapped Azure environment with 20+ segmented virtual networks for complete isolation.

Data Migration

100TB of database data migrated to Azure SQL Managed Instances with full redundancy and compliance controls.

Complete Security Stack

Defender XDR, Sentinel, Entra Domain Services, Intune, CIS Benchmarks, and Purview deployed across the environment.



Get a Security Operations Assessment from Bonelli Systems

Call for more information: 469-518-6987

Ask a question via email: sales@bonellisystems.com

Learn more at https://bonellisystems.com

18383 Preston Road, #202, Dallas, TX 75252

BONELLI SYSTEMS

Microsoft Solutions Partner
Data & AI Azure
Digital & App Innovation Azure
Infrastructure Azure
Security