
CONSULTING
PAIRING
HUMANS
AND
TECHNOLOGY

SECURING SERVER WORKLOADS WITH DEFENDER FOR SERVERS

CHALLENGES FACING SERVER SECURITY IN THE CLOUD-FIRST ERA

LACK OF VISIBILITY INTO SERVER THREATS

Missing telemetry across environments
Limited insight into threats on on-prem, multi-cloud, and disconnected servers.

No centralized inventory or health view
Difficult to assess the protection status of all workloads in one place.

NO CENTRALIZED ALERTING OR RESPONSE

Fragmented alert sources
Security signals scattered across disconnected tools and consoles.

Delayed incident response
No unified view to prioritize or act on critical threats in real-time.

INCONSISTENT SECURITY CONFIGURATIONS

Baseline drift over time
Manual configurations lead to deviations from security standards.

No enforcement of hardening policies
Lack of scalable controls for applying secure baselines consistently.

LIMITED AUTOMATION FOR REMEDIATION

Manual threat mitigation
Response actions depend on analyst intervention, delaying containment.

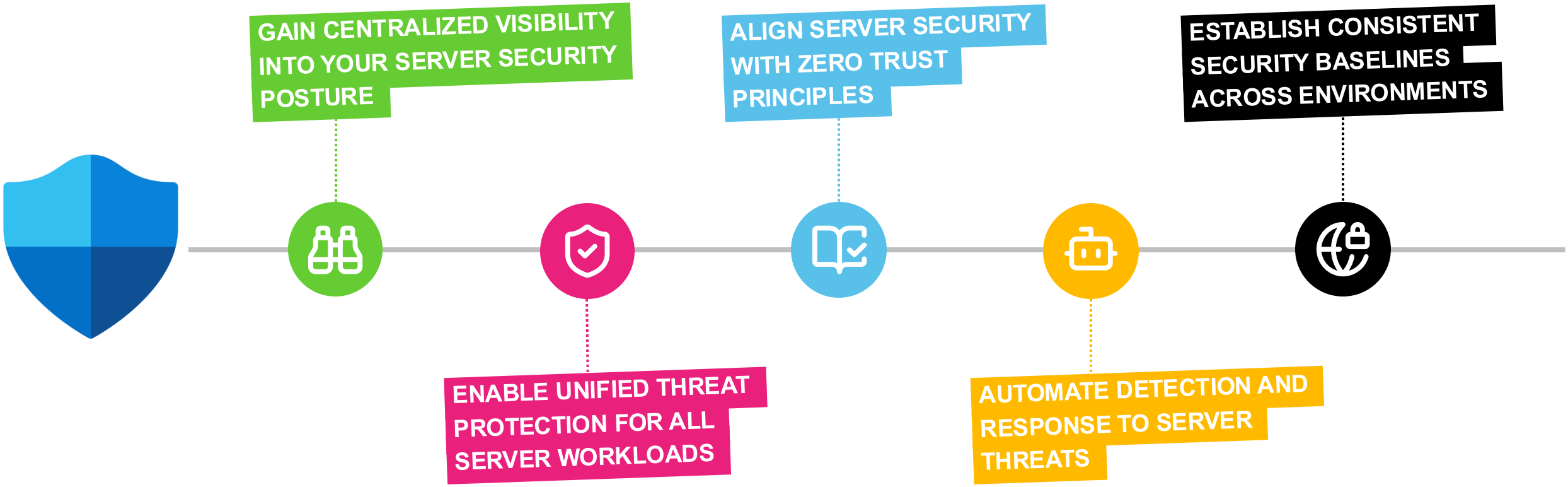
No auto-healing of misconfigurations
Security gaps persist due to lack of policy-driven remediation.

HYBRID SETUPS COMPLICATE PROTECTION

Diverse infrastructure
Servers span Azure, AWS, GCP, and on-prem, each with unique requirements.

Inconsistent tooling across platforms
Multiple agent stacks and consoles increase complexity and risk.

WHAT YOU'LL ACHIEVE WITH DEFENDER FOR SERVERS



CHOOSING THE DELIVERABLES FOR YOUR SCOPE

DEFENDER FOR SERVERS PLAN 1

EDR POWERED BY DEFENDER FOR ENDPOINT (PLAN 2)

- Endpoint detection & response (OS-level)
- Automatic on-boarding
- Next-generation antimalware
- Attack surface reduction rules
- Device control (USB)
- Network protection & web control
- Automated investigations
- Threat analytics
- Integrated incidents and alerts
- Advanced hunting
- Sandbox (deep analysis)

CORE VULNERABILITY MANAGEMENT FOR SERVERS

- Vulnerability assessment (agent-based)
- Configuration assessment
- Risk-based prioritization
- Remediation tracking
- Continuous monitoring
- Software inventory
- Software usage insights

DEFENDER FOR CLOUD FOUNDATIONAL POSTURE MANAGEMENT

- Regulatory compliance assessment for default compliance standards (i.e. Microsoft Cloud Security Benchmark (MCSB))

MULTICLOUD AND HYBRID SUPPORT

- Support for Azure, AWS and GCP VMs
- On-premises machines connected to Defender for Cloud

DEFENDER FOR SERVERS PLAN 2

PREMIUM VULNERABILITY MANAGEMENT FOR SERVERS

- Security baselines assessment
- Block vulnerable applications
- Browser extensions assessment
- Digital certificate assessment
- Network share analysis
- Hardware and firmware assessment

AGENTLESS SCANNING CAPABILITIES

- Threat detection (Azure network layer)
- Vulnerability scanning
- Malware scanning
- Machine secrets scanning

EXTENDED CAPABILITIES

- OS baseline misconfiguration
- OS system updates
- File integrity monitoring
- Just-in-time virtual machine access
- Network map
- Free data ingestion (500 MB Log Analytics)

PUTTING IT INTO ACTION

Discovery & Planning

- Assess server estate
- Define scope
- Select Defender plans (P1/P2)
- Align with stakeholders

Technical Enablement

- Integrate Defender XDR
- Define onboarding strategy
- Enable Defender for Cloud
- Prepare Windows security policies

Workload Onboarding

Establish capabilities to:

- onboard Azure servers
- onboard Arc-connected servers
- onboard AWS/GCP servers

Governance Foundations & Defender for Cloud Enablement

- Initial setup of Defender for Cloud (foundational CSPM)
- Define prerequisites and identify dependencies for CNAPP scale-up

Security Posture Assessment

- Review recommendations and secure score
- Analyse threat detections and misconfigurations
- Validate coverage and policy effectiveness
- Prepare improvement backlog

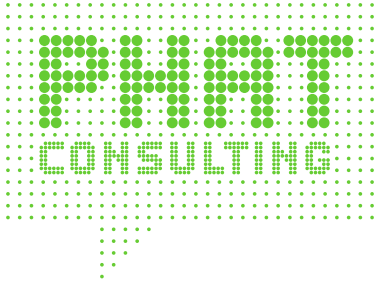
PUTTING IT INTO ACTION

	ESTIMATED EFFORT
Discovery & Planning	1-3 days
Technical Enablement	2-4 days
Governance Foundations & Defender for Cloud Enablement	2-5 days
Workload Onboarding	2-3 days
Security Posture Assessment	3-5 days
	10-20 days

DEFENDER IS LIVE – NEXT STEPS

- Implement settings management
- Implement a server update strategy
- Adopt cloud security benchmarks for servers
- Explore additional compliance standards
- Integrate with Microsoft Sentinel and SecOps
- Scale Defender for Cloud deployment and drive CNAPP adoption

WE LOOK FORWARD TO SEEING YOU
LET‘S GO!



PHAT CONSULTING GMBH
Nobistor 10 | 22767 Hamburg
040 226 383 - 100
info@phatconsulting.de