Professional Services for Ransomware Risk Mitigation

At a glance

Develop policies and processes to better defend against ransomware cyberattacks.

Key benefits

- Gain deep understanding of possible security risks and vulnerabilities to cyberthreats in your environment
- Improve your security posture with industry best practices to secure assets and ensure that your data is secure
- Learn about required countermeasures to reduce attack surfaces and minimize data risks

Business Challenge

Cyberattacks increased significantly in 2020 to the present with ransomware leading the way as one of the most frequent and devastating attacks, causing billions of dollars to organizations in recovery costs and ransoms paid.

Ransomware is a type of malware that sabotages organizations by encrypting their systems and data and deleting or encrypting their backups to negate recovery until a ransom is paid. Essentially, all valuables are held hostage for money.

Ransomware attacks can strike any organization in any industry anywhere around the globe, and the ease with which malicious actors can obtain ransomware compounds its proliferation.

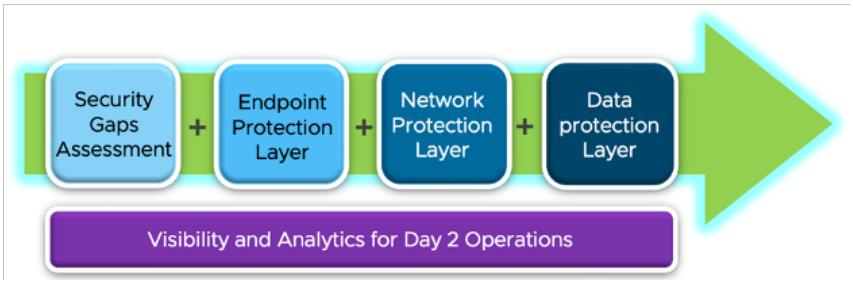
Preparation against ransomware attacks includes hardening defenses for cyberattacks by holistically securing business environments and empowering organizations with the knowledge, processes, and tools to prevent, detect, and respond to cyberthreats.

Service overview

When you work with VMware's Professional Services for Ransomware, our team will help you:

- Address the four layers of defense: security gaps assessment, endpoint protection, network protection, and disaster recovery protection
- Simplify the tools and processes required to secure end users and clouds
- Gain context and insights to accelerate how you identify risk and prevent, detect, and respond to cyberthreats

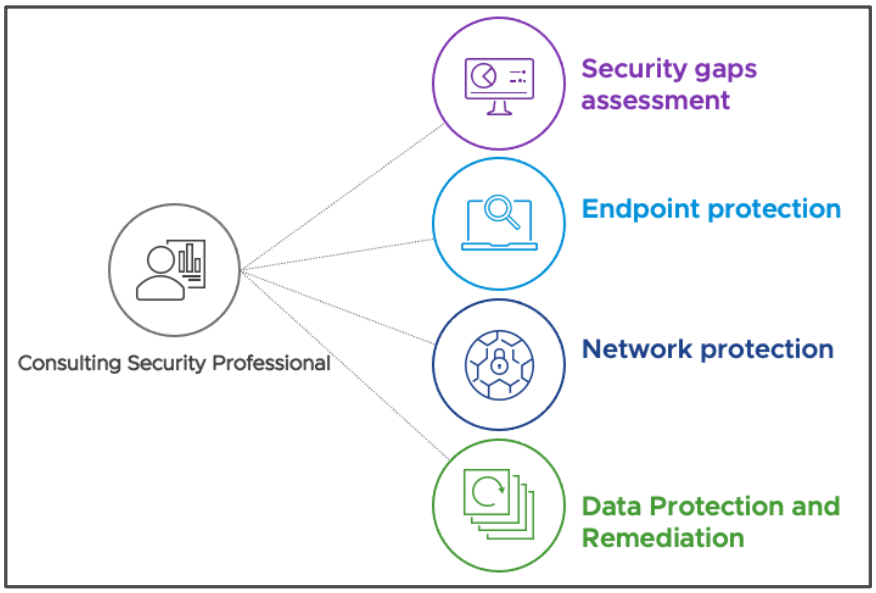
- Incorporate the National Institute of Standards and Technology (NIST) Cybersecurity Framework controls specific to the functions to protect, detect, and respond to cyberthreats
- Address customer use cases and requirements with modular solutions
- Learn about an end-to-end solution if needed



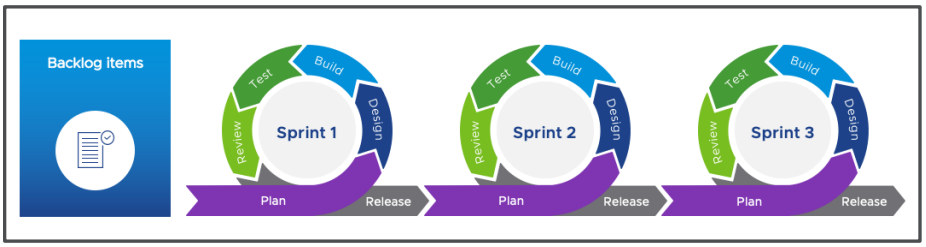
Service Engagement At-a-Glance

The VMware Professional Service for Ransomware follows an agile approach to protect the customer's infrastructure across four areas:

1. Understand current infrastructure and identify potential gaps or weaknesses
2. Endpoint protection best practices, guidance, and security configuration
3. Network protection best practices, guidance, and security configuration
4. Data protection and remediation processes



Services follow an incremental approach based on a set of agreed-upon activities with the customer. Tasks are accomplished with an agile approach of 2-week Sprints.

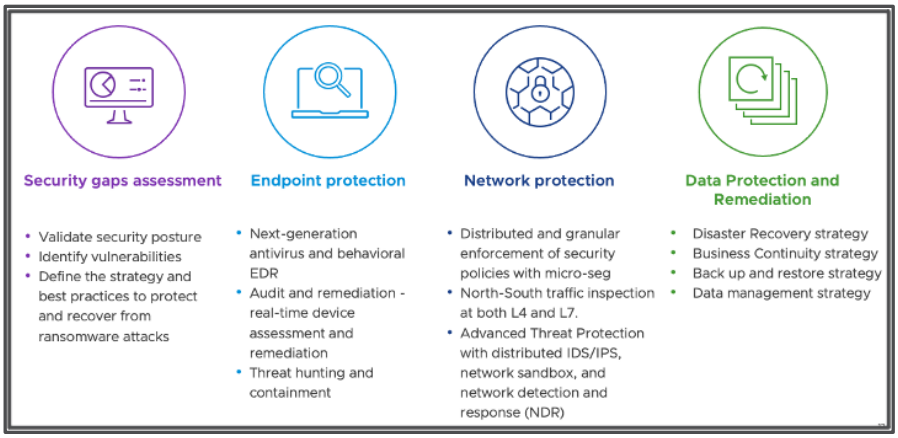


Deliverables

Based on service purchased, the customer will agree to a list of activities to be completed within the contracted duration of service. Minimum deliverables include a security gaps assessments and a Disaster Recovery strategy to adopt. Customers will receive reports describing existing gaps and misalignments and/or guidelines and best practices to adopt, to mitigate the risks and to equip the organization with Disaster Recovery plan to ensure the availability of data.

Customers will receive a both a presentation of prioritized recommendations with an overview of the current state, existing gaps, and next steps; moreover they will get a document with the guidance to implement the plan for the DR

Beyond guidance and recommendations, further services agreed to by the customer may include implementation of countermeasures to address security vulnerabilities found in the customer's environment, specifically around endpoint, network, or data protection. If Customer don't have yet the VMware Cloud Disaster Recovery, the VMware's Professional Services can provide the service to enable the DRaaS solution and implement the DR strategy for the set of workloads of their interest.



The delivery of the Ransomware Risk Mitigation service assumes the following:

- Carbon Black infrastructure is already deployed (if of interest for the customer)
- NSX infrastructure is already deployed (if of interest for the customer)

Service offering

The Ransomware Risk Mitigation service is an agile service that allows customers to choose the tasks to be completed for each 2-week Sprint from a predefined list of activities. Each of these options provides different areas of concentration.

The service will always include the security gaps assessment and the disaster recovery strategy; the recommended service duration to get anything done related to the backlog items requires a minimum of 6 Sprints. Customers can purchase additional concentration areas and tasks of interest and the overall engagement length will be augmented according to the specific customer scenario.

Customers can select any combination of the following:

- Security gaps assessment
- Endpoint protection
- Network protection
- Data protection and remediation

Hereafter, there is the list of service tasks, including the one included by default and the one optional task that can be added as part of the solution creation.

VMWare Security Service Tasks - backlog items		
Task	**Short Description**	**Included by default**
Security posture validation	Validation of key security controls available	Yes
Vulnerability identification	Perform security scrutinization seeking for weakness	Yes
Guidance on best practice against ransomware attack	provide a set of best practices to minimize the risk of being affected by a ransomware	Yes
Next-generation antivirus and behavioral EDR consumption	Leverage next-generation antivirus and behavioral EDR to protect endpoints	No
Audit and remediation consumption	Perform security audit and providing guidance for remediation	No
Threat hunting and containment consumption	Leverage threat hunting and containment for customer environment	No
Distributed firewalling with micro-seg policy definition and/or optimization	Distributed and granular enforcement of security policies with micro-seg consumption	No
Gateway firewalling policy definition and/or optimization	Distributed and granular enforcement of security policies with gateway firewall	No
Intrusion Detection/Prevention policy definition and/or optimization	Distributed and granular enforcement of security policies with IDS/IPS	No
Disaster Recovery strategy	Define and planning a DR strategy	Yes
Business Continuity strategy	Define and planning a BC strategy	Yes
Data Protection strategy	Define strategies and processes to secure the confindentiality, availability, and integrity of data	No
Introduction and Onboarding	Start up of activities, synch up with Customer	Yes

Learn more

Visit vmware.com/services.

Benefits

VMware consultants' knowledge and expertise will help you protect, detect, and respond to ransomware cyberattacks. When we help you with Professional Services for Ransomware, you will:

- Gain deep understanding of possible security risks and vulnerabilities to cyberthreats in your environment
- Improve your security posture with industry best practices to secure assets and ensure that your data is secure
- Learn about required countermeasures to reduce attack surfaces and minimize data risks