Enforce a Zero-Trust Ransomware Defense

Ransomware prevention and recovery for multi-cloud environments

○ Get Started

vmware®

The ransomware threat is real

The threat landscape continues to evolve, making ransomware defense a critical component of organizational resilience. An organization suffered a ransomware attack every 11 seconds in 2021, and it is expected that there will be a new attack on a consumer or business every two seconds by 2031[1]. According to the IBM Cost of a Data Breach Report 2022, the average cost of a ransomware attack (not including the ransom itself) is $4.54M[2] and 44% of intrusions perform lateral movement[3]. Paying the ransom has no guarantees — a staggering 96% of organizations who paid the ransom did not regain full access to their data[4]. As a result, the need for organizations to better protect and recover their data has become an urgent business imperative and a top CIO priority.

Cyber attackers are emboldened by the successes of ransomware. As enterprises adopt multiple clouds, the attack surface grows and inconsistencies in the operating model prevail to escalate the risk of cyberattacks, such as increasingly sophisticated ransomware attacks. Ransomware is an existential threat to organizations, exploiting weaknesses and inefficiencies in existing defenses. Once inside your data center, bad actors move laterally using legitimate ports and protocols and fileless techniques. When an attack happens, recovery is long and unpredictable due to the lack of automation in the many tools and processes involved. Enterprises must apply Zero-Trust principles to strengthen their ransomware defense. Customers need lateral security controls to detect anomalous behavior, contain and evict threats and an end-to-end recovery solution as a last line of defense.

Given the inevitability of ransomware attacks, the time is now to ensure your organization can defend itself and minimize any impacts a breach could have on your ongoing operations. This ebook details how **VMware can help you protect your multi-cloud environments with NSX Security and VMware Ransomware Recovery**, along with Professional Services, so you can reduce the risk of ransomware and outsmart cybercriminals.

[1] Cybersecurity Ventures
[2] IBM
[3] VMware Contexa
[4] Sophos

The entire ransomware attack lifecycle needs to be addressed

Breaching your organization is only the first step of a ransomware attack. Once in, an attacker will look to stay (persist) and learn about your environment to determine what and where your most valuable data is. In some cases, they may steal that data, in double and triple extortion attacks, before they encrypt it. Then, they will demand a ransom be paid in exchange for a decryption key that will return the data to its pre-attack state.

To truly minimize the threat of these increasingly prolific and destructive attacks, you need to be able to recognize and shut down all their different steps, vectors and impacts. This requires looking holistically at the entire attack lifecycle and building out capabilities that can mitigate the risks at each and every stage. The National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a way to start to think about and evaluate the types of capabilities you will need across the lifecycle:

Identify and understand the risks to your systems, assets, data, and capabilities.

Protect from known attacks by implementing appropriate controls and safeguards.

Detect actual attack activity.

Respond to contain and remediate an attack.

Recover and restore operations to pre-attack levels.

VMware can help you bolster your defenses across the ransomware attack lifecycle to improve your resilience and minimize the threat.

The ransomware threat is real ›

Enforce a zero-trust ransomware defense ›

Prevention ›

Recovery ›

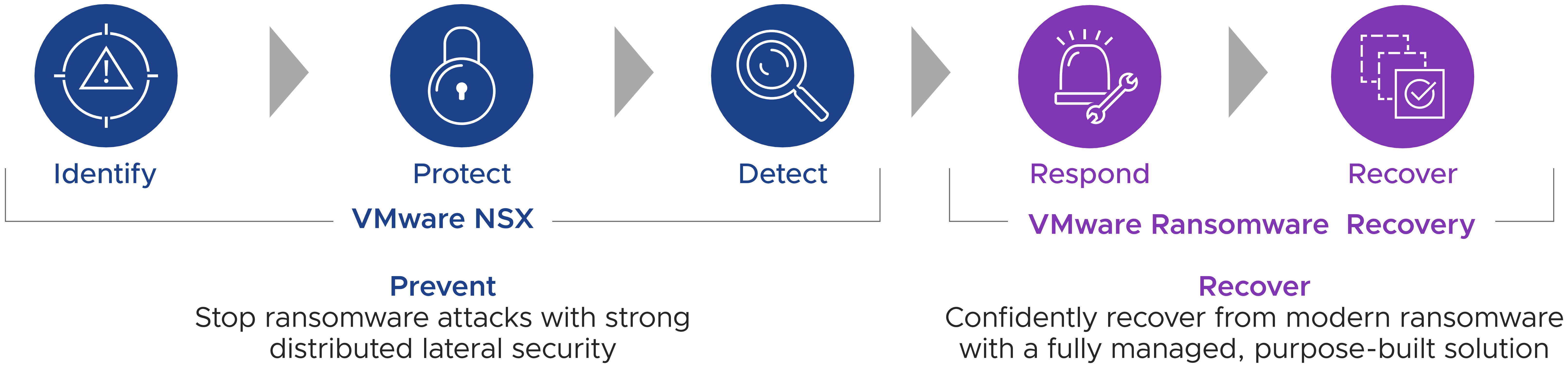
VMware professional services ›

VMware: providing coverage across the ransomware lifecycle

VMware solutions — **NSX Security and VMware Ransomware Recovery** — help you build the capabilities the NIST framework lays out to comprehensively combat ransomware (and other cyber risks). For example, you can protect all your workloads, endpoints, virtual desktop infrastructure (VDI), networks and containers, and get visibility and insights into every packet and process. This allows you to identify traffic (e.g., east-west, command and control (C2)) and payloads that are potentially malicious and then take action to contain or prevent them altogether. And you can ensure you are able to respond and recover from an attack quickly and seamlessly, so your business experiences little to no disruption.

VMware delivers a strong ransomware defense

Addressing the full ransomware protection cycle



Identify

Protect

Detect

Respond

Recover

VMware NSX

VMware Ransomware Recovery

Prevent
Stop ransomware attacks with strong distributed lateral security

Recover
Confidently recover from modern ransomware with a fully managed, purpose-built solution

The ransomware threat is real

Enforce a zero-trust ransomware defense

Prevention

Recovery

VMware professional services

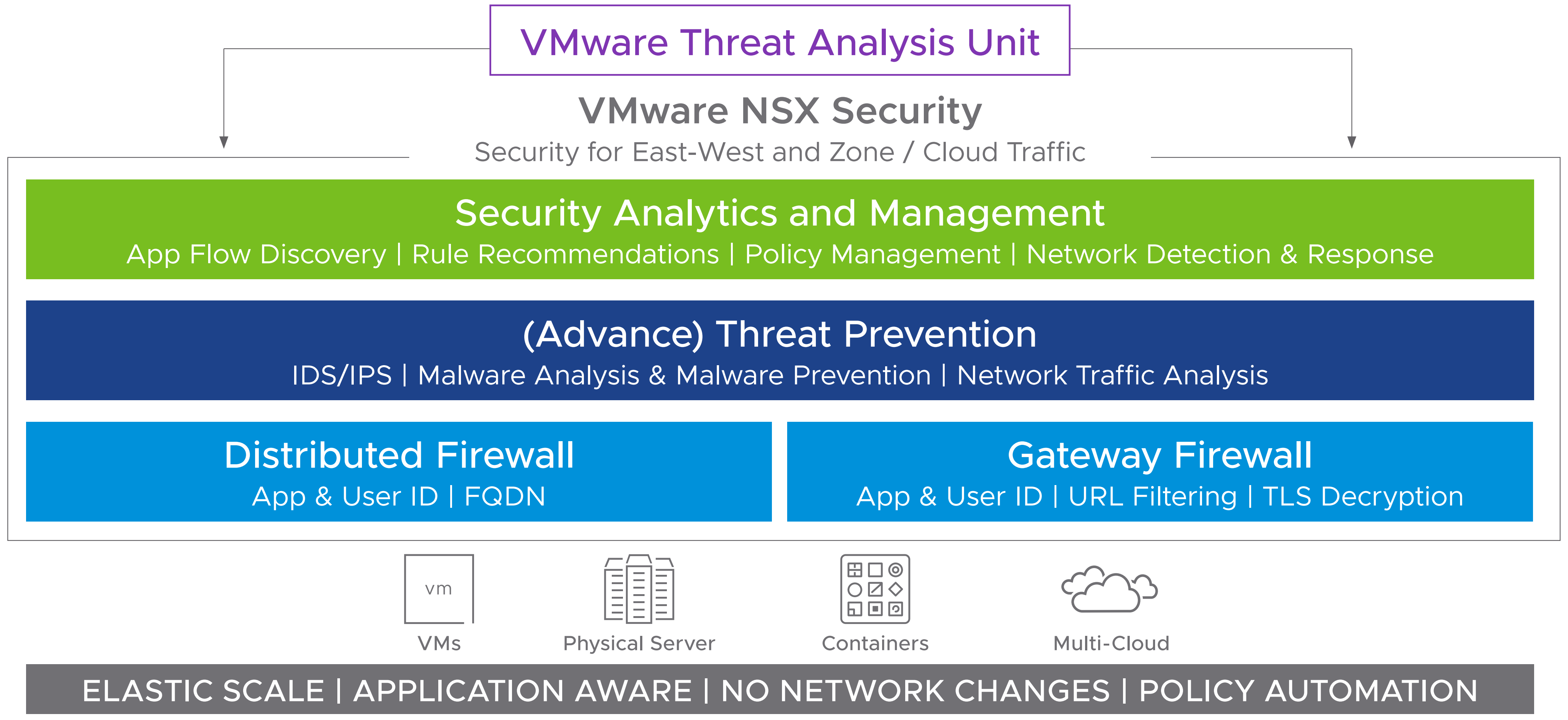
VMware NSX Security

VMware NSX Security enables you to manage your entire network security needs from a single pane of glass, allowing you to protect your applications across your data center, multi-cloud, and container infrastructure. The solution provides a software defined layer 2-7 firewall with IDS/IPS, sandboxing and NTA/NDR — distributed at each workload, simplifying the security architecture.

Unlike traditional firewalls that require network redesign and traffic hair-pinning, VMware NSX distributed architecture ensures no blind spots and the ability to scale, while providing visibility to every connection (Layer 4) and conversation (Layer 7). This enables you to segment the network, stop the lateral movement of attacks, and automate policy in a simpler operational model.

As the industry's first and only SE Labs AAA-rated network detection and response solution with 100% detection rate, VMware delivers a strong ransomware defense with lateral security that enables you to find and evict threat actors in your network.

Visibility & enforcement across the attack chain
Access control + ATP + analytics and management



VMware Threat Analysis Unit

VMware NSX Security

Security for East-West and Zone / Cloud Traffic

Security Analytics and Management

App Flow Discovery | Rule Recommendations | Policy Management | Network Detection & Response

(Advance) Threat Prevention

IDS/IPS | Malware Analysis & Malware Prevention | Network Traffic Analysis

Distributed Firewall

App & User ID | FQDN

Gateway Firewall

App & User ID | URL Filtering | TLS Decryption

VMs

Physical Server

Containers

Multi-Cloud

ELASTIC SCALE | APPLICATION AWARE | NO NETWORK CHANGES | POLICY AUTOMATION

Key advantages:

- **Get complete network security coverage** across all traffic flows and workload types to make sure nothing is missed.
- **Easily create, enforce, and manage granular micro-segmentation policies** to secure the East-West traffic and make it difficult for attackers to persist.
- **Analyze advanced threats** with a full-system emulation sandbox, so you know exactly what you are dealing with and can take appropriate steps to respond.
- **Quarantine infected guests** to **prevent lateral attack movement** and prevent attack propagation.

The ransomware threat is real >

Enforce a zero-trust ransomware defense >

Prevention >

Recovery >

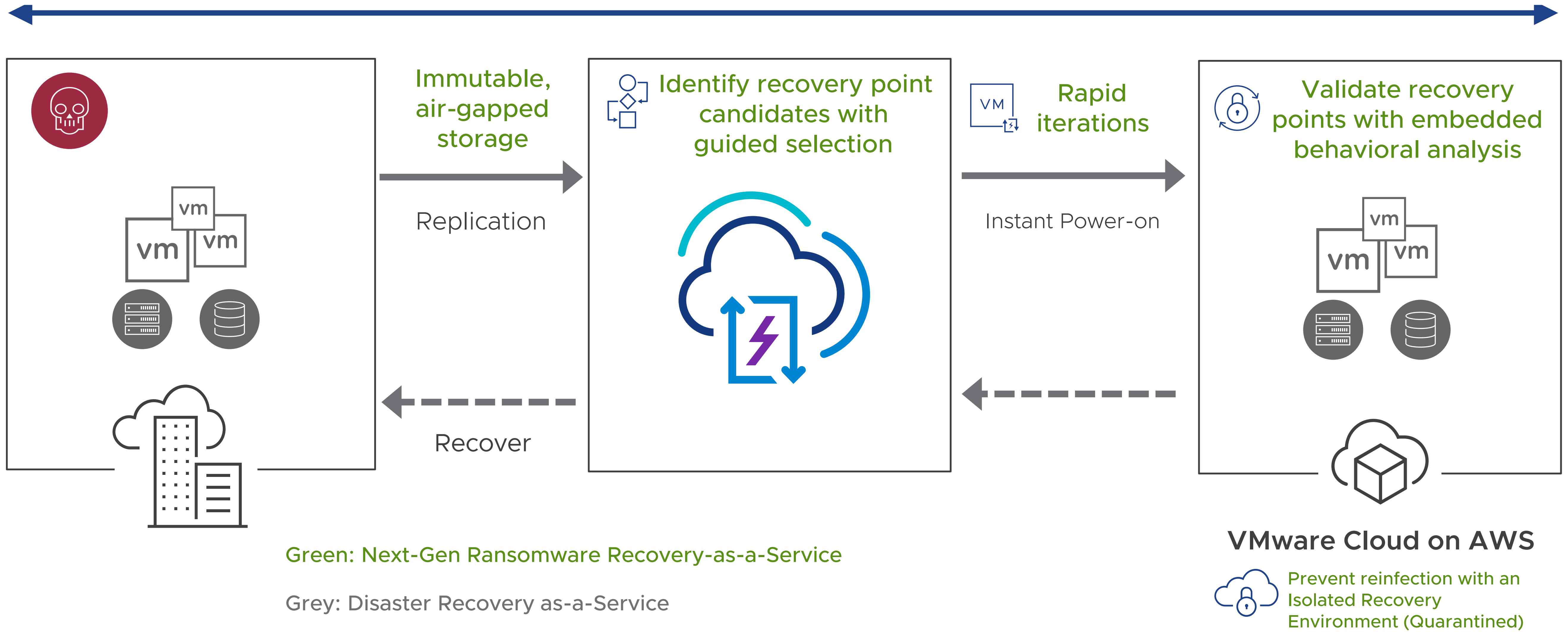
VMware professional services >

Recovery from modern ransomware

VMware Ransomware Recovery is a fully managed Ransomware Recovery-as-a-Service solution that enables safe recovery from modern ransomware through behavioral analysis of powered-on workloads in an Isolated Recovery Environment (IRE) in the cloud. Guided workflow automation allows customers to quickly identify recovery point candidates, validate restore points using live behavioral analysis, and prevent reinfection with networking isolation capabilities.

VMware ransomware and disaster recovery

Purpose-built, fully managed ransomware and disaster recovery, delivered as an easy-to-use SaaS solution



Immutable, air-gapped storage

Replication

Recover

Identify recovery point candidates with guided selection

Rapid iterations

Instant Power-on

Validate recovery points with embedded behavioral analysis

VMware Cloud on AWS

Prevent reinfection with an Isolated Recovery Environment (Quarantined)

Green: Next-Gen Ransomware Recovery-as-a-Service

Grey: Disaster Recovery as-a-Service

Key advantages:

Confident recovery from existential threats:

- Fully-managed, cloud-based Isolated Recovery Environment (IRE)
- Embedded behavioral analysis of powered-on workloads to identify, contain and eradicate modern strains of ransomware from recovery points

Quick recovery with guided automation:

- Step-by-step, guided ransomware recovery workflow streamlines and automates recovery operations
- Push-button VM network isolation levels to prevent lateral movement of ransomware at recovery which could lead to reinfection

Simplified recovery operations:

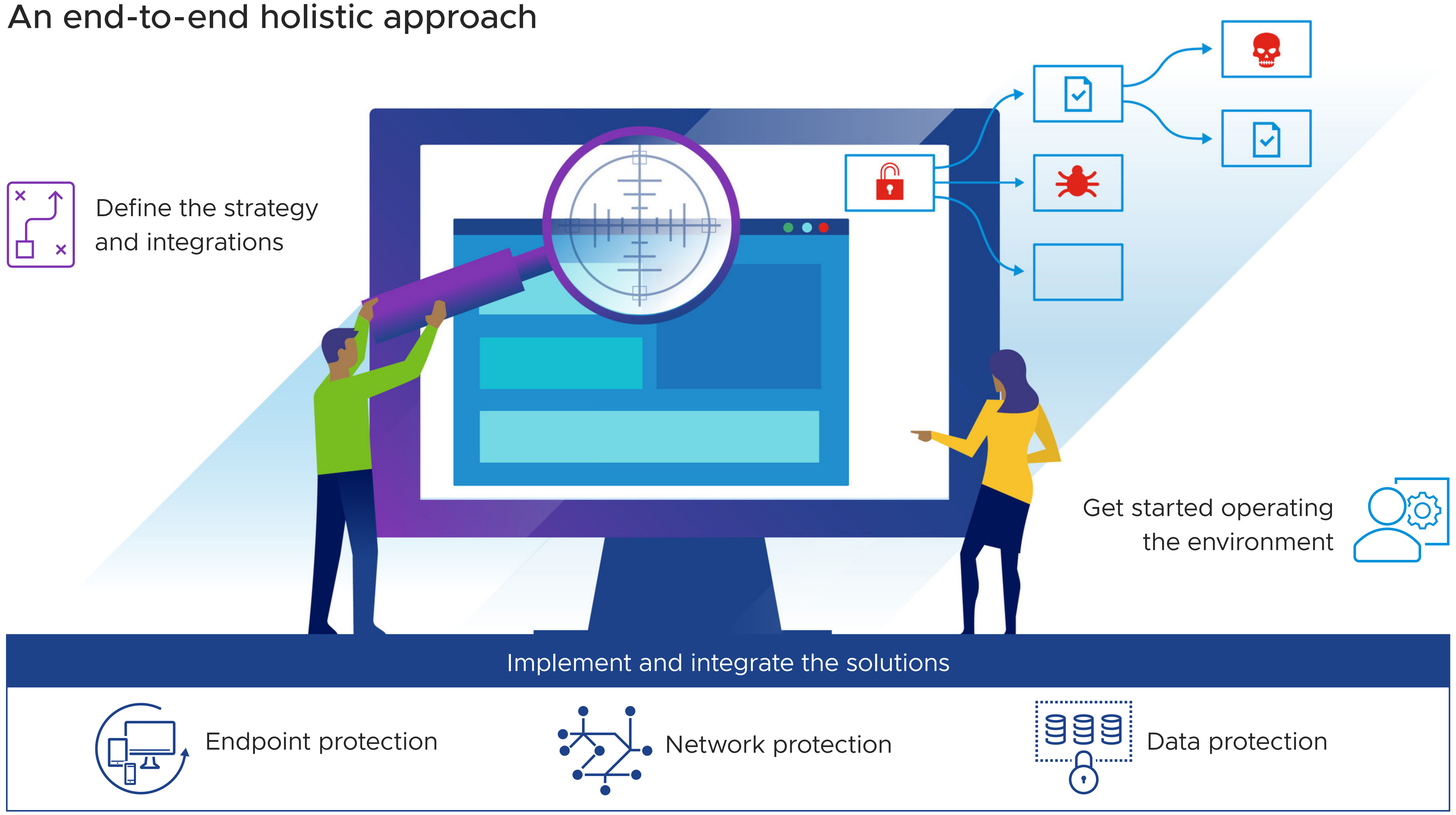
- Integrated availability, security and networking into a single solution to address the entire ransomware recovery operation
- Boost collaboration between Security and Infrastructure teams

VMware professional services

VMware Professional Services help you implement a holistic solution to mitigate ransomware attacks. They start by defining a tailored strategy that takes into account all your endpoint, network, and data protection needs. They provide product configurations and integrations, as well as guidance for security countermeasures and operating procedures, so you can streamline product implementation and management.

Ransomware risk mitigation implementation methodology

An end-to-end holistic approach


Define the strategy and integrations
Get started operating the environment
Implement and integrate the solutions
Endpoint protection
Network protection
Data protection

Key advantages:

- **Speed up the implementation** of your ransomware risk mitigation strategy and solution, so you can reduce the risk and impact of a successful attack.
- **Better prepare to recover** in the event of an attack to minimize any disruptions to existing resources and operations.
- **Improve security operations** through knowledge transfer, operational guidance, and standard operating procedures that help you establish and follow best practices.
- **Minimize the risk of ransomware** with a proven approach and expertise that helps you appropriately address all phases of the attack lifecycle.

Summary: protect your business from modern ransomware

Ransomware attacks will continue to be increasingly prolific and destructive, until organizations can holistically address the threat and make it harder for attackers to succeed at any phase. This takes a comprehensive approach, like the one VMware offers to help you:

- **Identify** and address the risk of ransomware across all your environments.
- **Prevent** malicious activity with granular controls and safeguards, such as segmentation/micro-segmentation, that stop attacks before they can even get started.
- **Detect** attack activity, including lateral movement and other advanced tactics, so action can be taken to shut them down and ensure an attacker cannot persist.
- **Respond** fast to fully contain and remediate an attack to eliminate it from your environment.
- Quickly **Recover** and restore operations to minimize any impacts on your business.

Learn more

Join us online: