Reducing Your Ransomware Risk

How VMware Helps Protect Your Multi-Cloud Environments Against Ransomware

Get Started

vmware®

The Ransomware Threat is Real

Ransomware attacks made *headlines in 2021*, crippling critical infrastructure and disrupting the operations of a number of high-profile companies. *Cybersecurity Ventures* predicts that every 11 seconds a business is hit by a ransomware attack. Our own *2021 Global Security Insights Report* identified ransomware as the "second most common vector that caused breaches".

Cyber attackers have been emboldened by ransomware's success. They've been doubling down and investing in building out their capabilities to launch even more devastating attacks. Many are taking advantage of the burgeoning Ransomware-as-a-Service (RaaS) market to increase their speed and reach—an attack can now be launched in just three clicks. A recent international partner *advisory* jointly issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), confirmed the threat of ransomware attacks is only expected to grow and get worse in the coming months.

Given the inevitability of ransomware, 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 Carbon Black Cloud, NSX Security, and VMware Cloud Disaster Recovery, along with Professional Services, so you can reduce the risk of ransomware and start to get the upper hand on attackers.

The Entire Ransomware Attack Lifecycle Needs to be Addressed

Getting into 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.

Prevent known attacks by implementing appropriate controls and safeguards.

Detect actual attack activity.

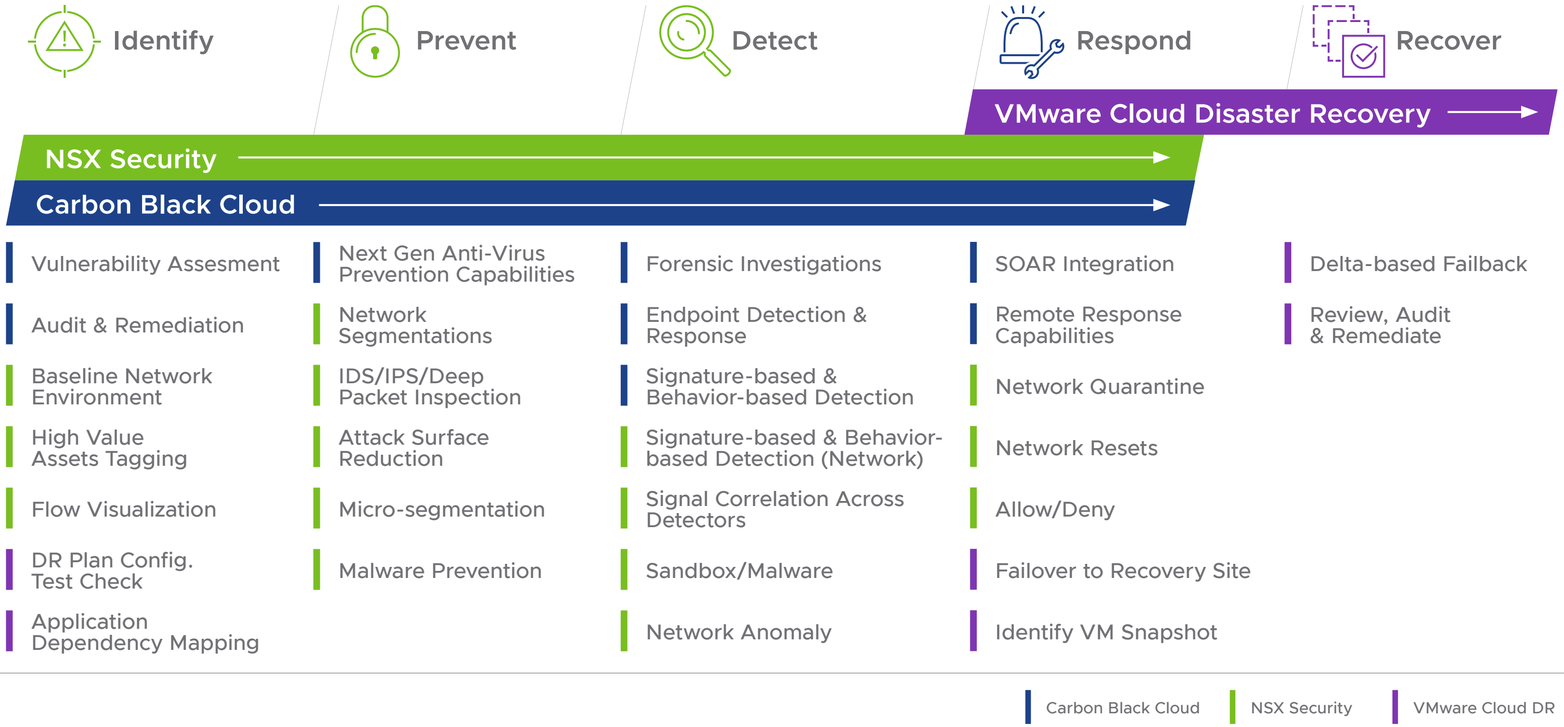
Respond to contain and remediate an attack.

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.

VMware: Providing Coverage Across the Ransomware Lifecycle

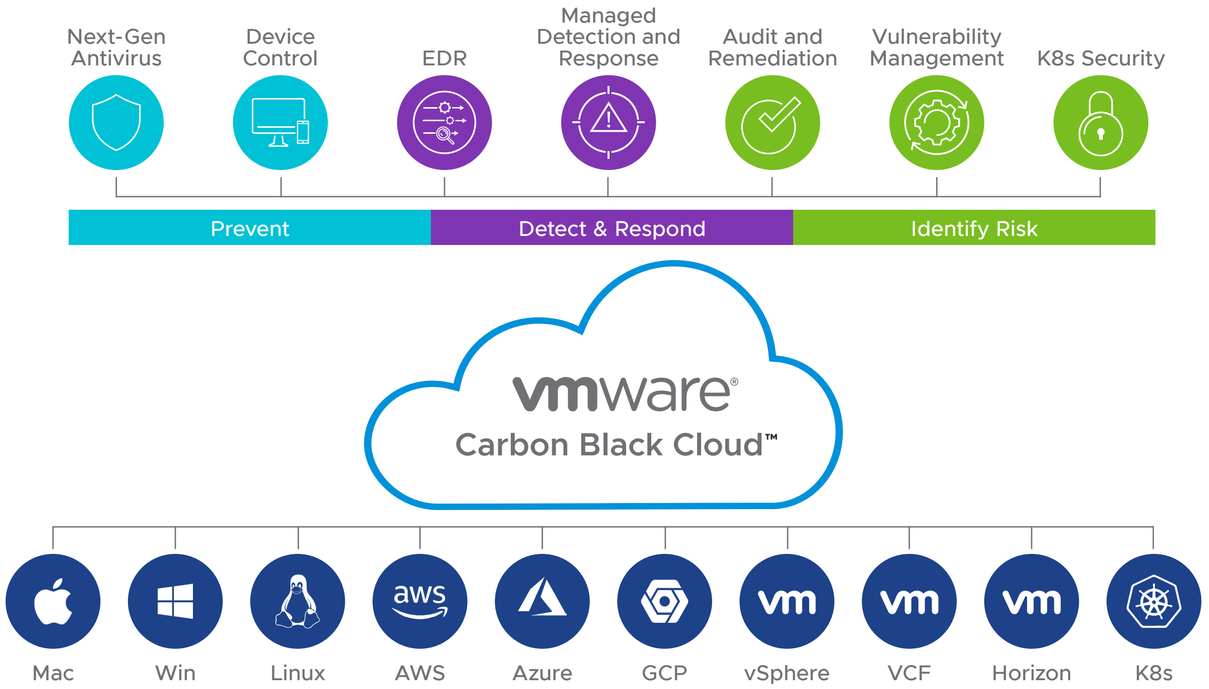
VMware solutions - **VMware Carbon Black Cloud, NSX Security, and VMware Cloud Disaster Recovery –** help you build the capabilities the NIST framework lays out to comprehensively combat ransomware (and other cyber risks). For example, you can protect all your workloads, endpoints, virtual desktop infrastructure (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 Carbon Black Cloud

VMware Carbon Black Cloud provides next-generation anti-virus (NGAV), endpoint detection and response (EDR), advanced threat hunting, vulnerability management, rollback capabilities, and more to enable you to reduce your attack surface and protect your critical assets against attack. With Carbon Black Cloud, you get multiple layers of prevention, robust visibility, and response capabilities you can use to protect your environment from the threat of ransomware.

Carbon Black Cloud Platform Overview



Key Advantages for Ransomware Protection:

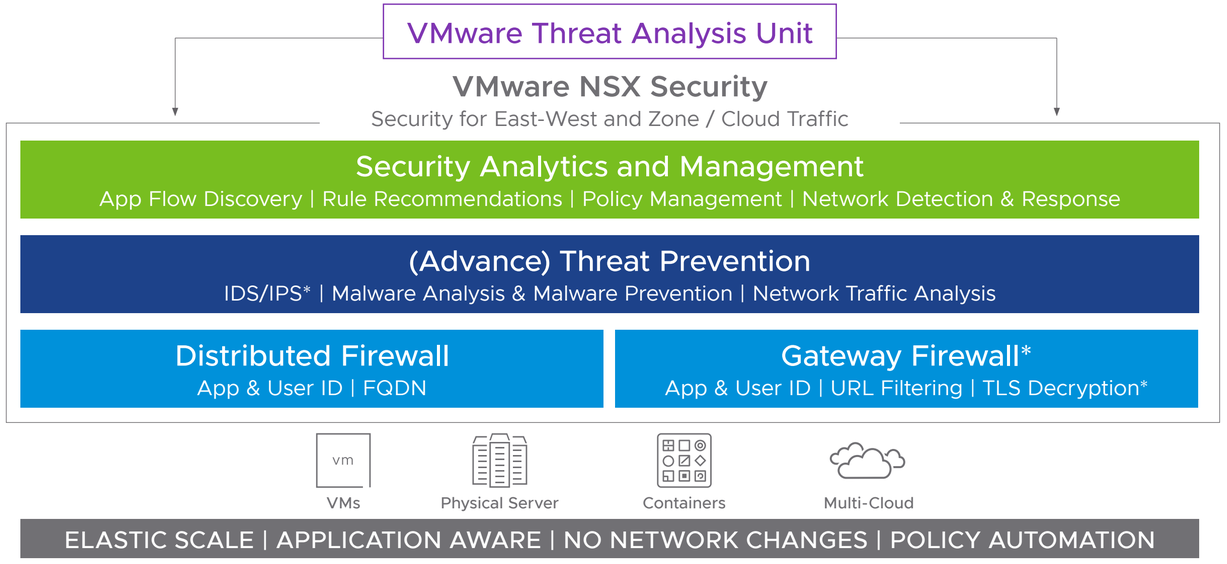
- Implement a **multi-layered prevention approach** that protects against advanced threats, such as ransomware, with the ability to **detect malicious activity** at different stages of an attack.
- Take advantage of **built-in response capabilities that decrease time to resolution** and minimize any attack impacts.
- **Search and filter across all events** in your environment for the past 30 days to make sure you have the data you need for investigations and can fully remediate an attack.
- Get an easy-to-understand **view of events, with alert visualizations**, that show everything that occurred, so you can take steps to ensure attackers can't persist.

VMware NSX Security

VMware NSX Firewall enables you to manage network security for the entire network from a single pane of glass, so you can quickly protect your applications across your data center, multi-cloud, and container infrastructure. The solution provides a software-defined layer 2-7 firewall at each workload. This makes it easy to deliver granular protection with network segmentation and micro-segmentation, so that if (or when) an attacker gets into your network they are extremely limited in where they can go and what they can do. You can also create context-aware security policies and leverage advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), network traffic analysis / network detection and response (NTA/NDR), and network sandboxing to further defend against lateral threats.

Visibility & enforcement across the attack chain

Access Control + ATP + Analytics and Management



* IDPS AND TLS Decryption on GFW is Tech Preview only in NSX-T 3.2

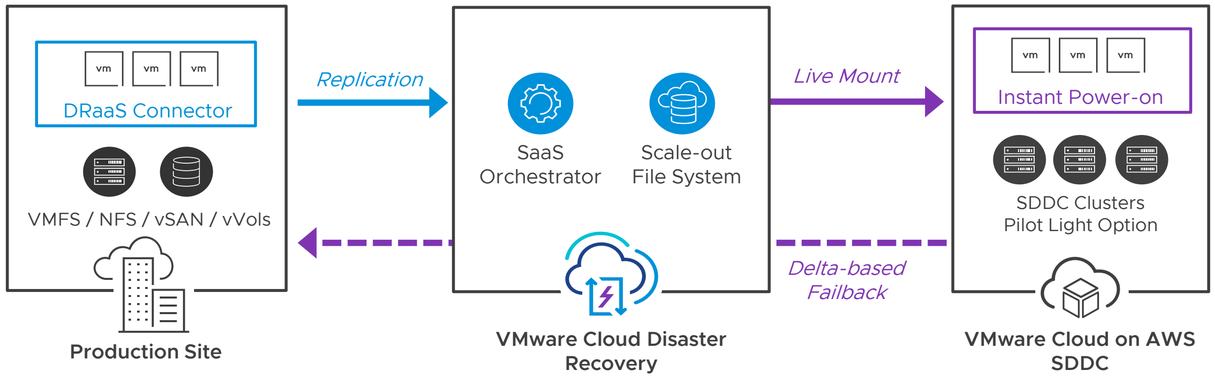
Key Advantages for Ransomware Protection:

- 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.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery delivers on-demand ransomware and disaster recovery, delivered as an easy-to-use SaaS solution, with cloud economics. It combines cost-efficient cloud storage with simple SaaS-based management to deliver IT resiliency at scale, through simple DR testing, orchestration of failover and failback plans and streamlined ransomware recovery. Customers benefit from a 'pay when you need' failover capacity model for DR resources.

Protect your datacenter to the cloud with VMware Cloud Disaster Recovery



Blue: Steady-state operations
Purple: Activated for tests, failovers, failbacks

Key Advantages for Ransomware Recovery:

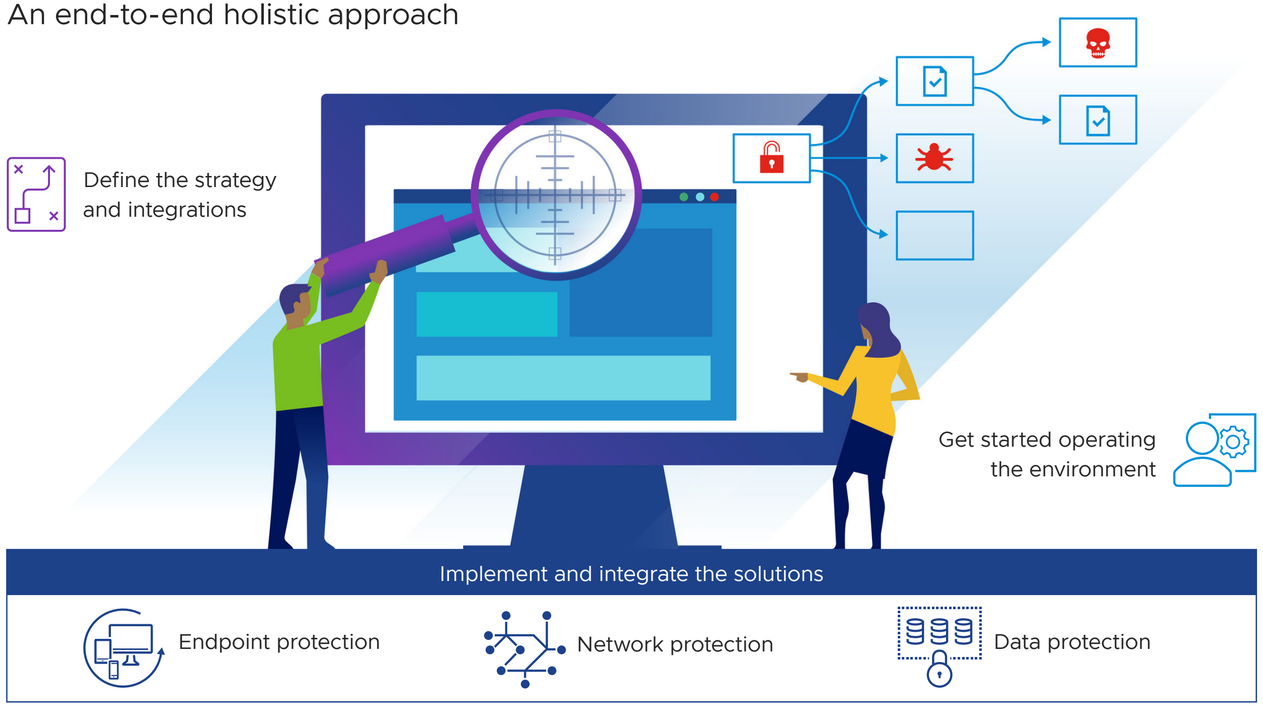
- Use **offsite air-gapped backups** to reduce the direct impact of attack.
- Ensure previous clean recovery points can't be altered by malware with **immutable VM snapshots and data integrity features**.
- Benefit from recovery point objectives **(RPOs) as low as 30 minutes**, as well as a **deep history of snapshot copies** to increase your overall resilience.
- Use an on-demand software-defined data center (SDDC) in the cloud for **Instant Power-On of VMs** that minimize any disruptions.
- Utilize the **granular recovery capability** to extract individual files and folders from recovery points without powering VMs on, and merge them into a final recovery point to **minimize data loss** at recovery.
- **Non-disruptively test** your DR plans

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.

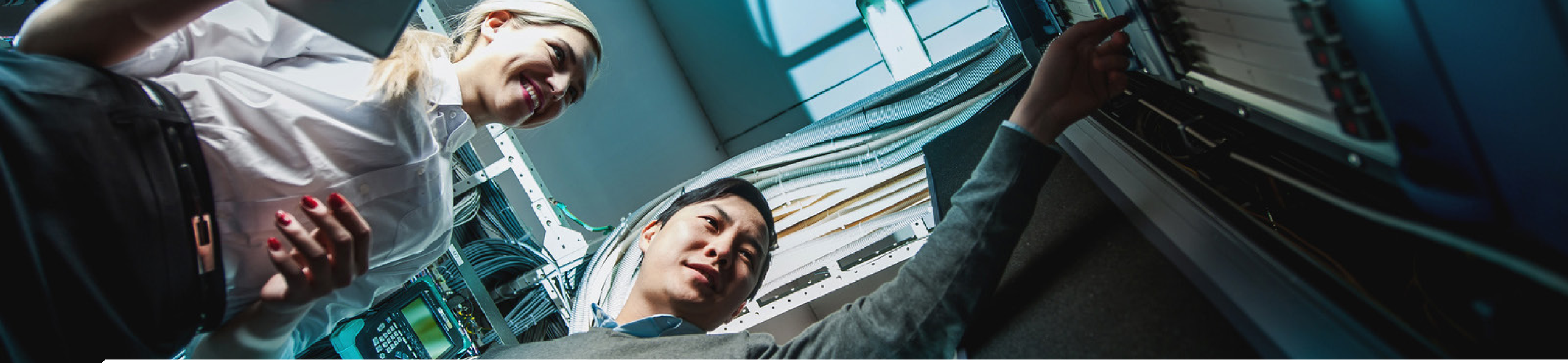
Rasomeware risk mitigation implementation methodology

An end-to-end holistic approach



Key Advantages for Ransomware Risk Mitigation:

- **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 Organization from the Ransomware Threat

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: