

EBOOK

# CODE RED ALERT: DON'T BECOME THE NEXT DIGITAL HOSTAGE

Best Practices for  
Ransomware Prevention  
and Mitigation



# The Ransomware Blues.

**Despite recent crackdowns, ransomware continues to be major threat.**

Ransomware is a type of malware that encrypts files or locks users out of devices and systems with the intent that after the organization makes payment, access will be restored. According to [Chain Analysis](#), ransomware payments exceeded \$1 billion in 2023.

Furthermore, the 2024 Verizon Data Breach Investigations Report found that “roughly one-third of all breaches involved ransomware or some other extortion technique...and ransomware was a top threat across 92 percent of industries.”

In recent months, a coordinated effort across several law enforcement agencies [resulted in several arrests](#) of one of the major ransomware players, LockBit. However, these actions have not had any impact on the volume of attacks. Ransomware continues to be a threat. But don't panic! In this eBook, we will highlight some best practices to protect your organization.

Ransomware is a **growing threat**. But don't panic! In this eBook, we will highlight some **best practices to protect your organization**.



According to the 2024 Astra Blog, **92% of malware is delivered through email.**

# The Challenges of Ransomware.

**As a form of malware, ransomware can be delivered in a variety of ways, including common attack vectors such as phishing emails, malicious downloads, and unsafe websites.**

According to the [2024 Astra Blog](#), 92% of malware is delivered through email. Additionally, the 2024 IBM Cost of a Data Breach Report found that “the share of breaches caused by ransomware grew 41 percent in the last year and took 49 days longer than average to identify and contain.” However, we have also noticed a trend towards ransomware attacks targeting servers directly, so it is not just your endpoints at risk!

The primary challenges of ransomware are:

- Signature-based tools find it difficult to detect new threats and techniques.
- Machine learning and reputation-based tools are not effective in “living off the land” techniques.
- Endpoint detection and response tools require human investment to triage events.

While all of these tools are useful and necessary, they need to be complimented by other technologies to address the ransomware threat. This eBook will highlight some of these other tools.

# Breaking the Lock.

**There is no silver bullet when it comes to combating ransomware attacks. It takes multiple security technologies and approaches working together to help prevent and mitigate this threat.**

Here are six tips that you can incorporate into your security strategy to help safeguard your organization against ransomware and other email-based attacks.

1. **Heading Attacks Off at the Pass.** Implement comprehensive email security to inspect and block suspicious emails and links from entering your user's inboxes.
2. **The Best Offense is a Good Defense.** Install reputable antivirus software with real-time protection to catch malicious emails that slip through your email security.
3. **An Apple a Day Keeps the Hacker Away.** Keep your endpoints updated and patched. Many attackers exploit known vulnerabilities to compromise laptops and servers.
4. **Take a Photograph, It Lasts Longer.** Back up your files regularly to the cloud or external drives to ensure that any data that gets compromised can be quickly recovered.
5. **Extend Zero Trust to the Kernel.** Create and enforce policy controls over users, accounts, and systems that have elevated or privileged entitlements.
6. **Lock Away Your Heart.** Encrypt all sensitive data to keep hackers from accessing and stealing it, and implement remote wiping to destroy any data that falls into their hands.

Here are **six tips** that you can incorporate into your security strategy to **help safeguard your organization** against ransomware and other email-based attacks.





An intelligent, comprehensive email security platform **stops spam and malware** with technologies such as reputation analysis, antivirus engines, and antispam signatures.

# Heading Attacks Off at the Pass.

**Email is the most common way for cyber criminals to launch and distribute threats.**

Advanced email threats such as spear phishing, ransomware, and business email compromise scams are now favored because these attacks use domain spoofing and obfuscation to hide malicious links, making them far more difficult to detect and stop than traditional malware. As a result, standard signature-based antimalware tools have proven largely ineffective against them.

Symantec® Email Security.cloud enhances the native security of email systems, effectively preventing malware and email threats with minimal false positives. Additionally, Symantec Email Threat Detection Response and Isolation extends these capabilities by incorporating advanced technologies such as cloud-based sandboxing, click-time URL protection, Office365 clawback, and web browser isolation with telemetry from the Symantec Global Intelligence Network (GIN) to block sophisticated attacks such as ransomware, spear phishing, and business email compromise (BEC). Combined, these cloud-based services provide an intelligent, comprehensive email security platform.



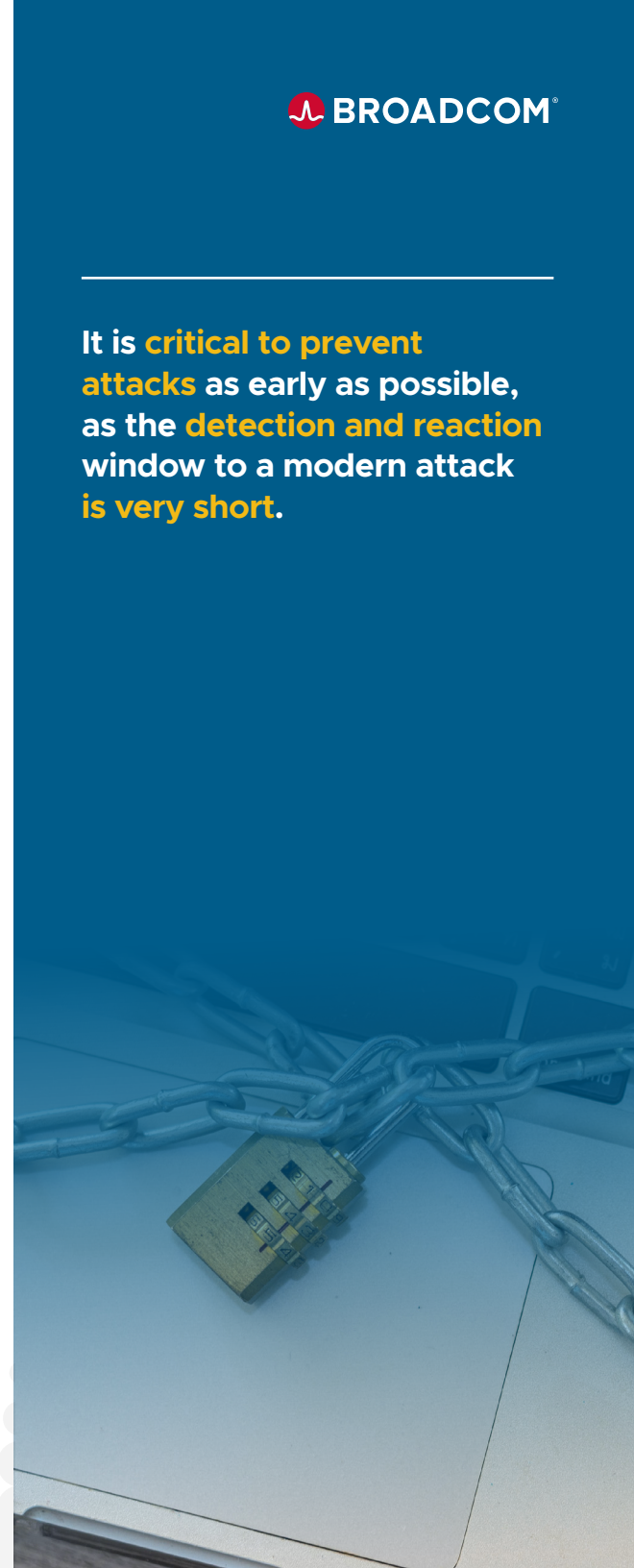
# The Best Offense is a Good Defense.

**Endpoint Security is still one of the most critical lines of defense in preventing cyber attacks from compromising devices.**

Prevention matters as global cyber threats are more aggressive than ever and can have a staggering impact on a business. It is critical to prevent attacks as early as possible, as the detection and reaction window to a modern attack is very short. A comprehensive and integrated endpoint security solution protects traditional and mobile endpoints, providing interlocking defenses at the device, application, and network levels.

Symantec Endpoint Security delivers an innovative adaptive protection approach to help organizations shift left and focus on enhancing protection across the entire attack chain—with an emphasis on prevention for rapid containment. Beyond the basics—antivirus, spam, and malware protection, the solution also leverages AI to optimize security decisions and sandboxing to detect malware hidden in custom packets.

It is **critical to prevent attacks** as early as possible, as the **detection and reaction** window to a modern attack is **very short**.





---

Astra Security found that “**nearly half of all businesses do not have a vulnerability management program in place to identify and fix security vulnerabilities before they can be exploited.**”

# An Apple a Day Keeps the Hacker Away.

**As of January 24, 2024, the National Vulnerability Database maintained by the National Institute of Standards listed 236,489 vulnerabilities.**

The most successful attacks exploit known vulnerabilities on endpoints that were not properly configured or patched. These weaknesses exist because many organizations lack real-time visibility into the state of their own endpoints. In fact, Astra Security found that “nearly [half of all businesses](#) do not have a vulnerability management program in place to identify and fix security vulnerabilities before they can be exploited.”

Symantec IT Management Suite enables you to meet this challenge by securely managing devices both inside and outside the perimeter. The solution improves your security posture by providing visibility into the hardware and software in your environment, as well as identifying and remediating vulnerabilities through robust patch management capabilities across a wide variety of endpoints.





# Take a Picture, It Lasts Longer.

**The recovery time from a ransomware attack can be significantly reduced if you have a copy of the data stolen or encrypted.**


The real threat from ransomware is the encryption of files and/or blocking access to devices and systems, and the payment demanded is predicated on the need to have this access restored. If, however, the organization regularly backs up their files to the cloud or an external drive, then the hacker-encrypted data can be easily recovered without making any payments to the criminals.

Similarly, organizations can also restore systems that are compromised by a ransomware attack. VMware Live Cyber Recovery provides a purpose-built ransomware recovery-as-a-service offering that can assist organizations to overcome the [top five challenges in ransomware recovery](#).

---

VMware Live Cyber Recovery™ provides a **purpose-built ransomware recovery-as-a-service offering** that can assist organizations overcome the **top five challenges in ransomware recovery**.





Symantec PAM **provides server control agents** that enable organizations to centrally administer all aspects of host server security.

# Extend Zero Trust to the Kernel.

**Enforcing fine-grained access controls at the kernel level can prevent ransomware attacks that target servers with living off the land tools.**

Ransomware attackers are shifting to Internet-facing server and device vulnerabilities, which is leading to low dwell times and the need for proactive prevention and not after-the-fact detection and response. However, the usage of dual-use and living off the land tools makes identification and prevention more difficult. Fine-grained access controls at the kernel level can thwart this attack vector.

Symantec PAM is a comprehensive solution designed to prevent security breaches by providing robust privileged access management capabilities. To help address direct ransomware attacks on servers, it offers server control agents that enable centralized administration of host server security. These agents, operating at the kernel level, enforce stringent controls—even when attackers gain root-level access. Through these policy enforcement points, Symantec PAM restricts malicious activities that are often performed by these ransomware attackers, such as accessing sensitive files, executing unauthorized commands, installing programs, altering log files, or establishing unauthorized network communications.

# Lock Away your Heart.

**A comprehensive data encryption strategy assists with data privacy compliance and helps qualify for safe harbor.**

This may be hard to believe but criminals cannot be trusted. Shocking! While demanding ransom to return your data, hackers will often access and steal that data to sell on the open market. This can be prevented by having all data encrypted before a successful ransomware attack.

Symantec Encryption provides flexible data-at-rest protection across end-user devices, internal servers, and third-party cloud environments. This addresses the theft of data from a ransomware attack by making it inaccessible to criminals. But this capability can be further enhanced using remote wipe, which allows security administrators to erase all data on a compromised endpoint at the touch of a button; thereby eliminating the data from the hacker's control.

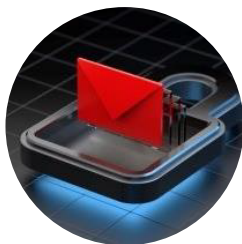
**A comprehensive encryption solution provides flexible data-at-rest protection across end-user devices, internal servers, and third-party cloud environments.**



Broadcom offers  
comprehensive  
**ransomware protection**  
for the entire enterprise.

# The Symantec Portfolio.

Introducing the Ransomware Security Portfolio by Symantec.



## Symantec Email Security

Protect email messages against threats, user error, and data leakage



## Symantec Endpoint Security

Safeguard traditional and mobile devices with innovative technologies



## Symantec Endpoint Management

Remediate vulnerabilities through automated patch management



## Symantec Privileged Access Management

Enforce controls over system-level access and privileged user actions



## Symantec PGP Encryption

Encrypt sensitive data to prevent theft and address regulatory compliance

**ARE YOU DOING  
ENOUGH TO PROTECT  
YOUR DATA FROM  
RANSOMWARE?**

Broadcom offers the  
**following competitive  
advantages** to help  
protect your data.



# Why Broadcom

## Three reasons to partner with us.

**Broadcom offers three differentiators over the competition when considering a vendor to help protect your data.**

### MOST SECURITY



Broadcom cybersecurity solutions safeguard data at every stage of their lifecycle.

### MOST COVERAGE



Broadcom cybersecurity bridges the hybrid environments to safeguard data everywhere.

### MOST TRUSTED



Broadcom cybersecurity has protected the world's largest customers for over 50 years.



For more information, please visit our website at: [www.broadcom.com](http://www.broadcom.com)

Copyright © 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

**Code Red Alert: Don't Become the Next Digital Hostage eBook January 28, 2025**