Trend Micro

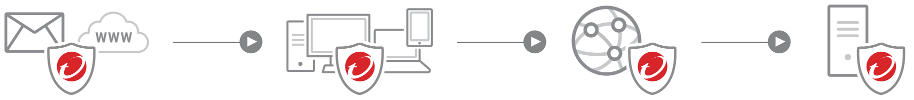
PROTECT YOUR ORGANIZATION FROM THE UNFORESEEN IMPLICATIONS OF RANSOMWARE

Ransomware has rapidly emerged as a significant threat to businesses and organizations of all sizes. In this day and age where data is invaluable, cybercriminals are taking advantage of people who don't know a lot about malware behavior.

You need a plan to minimize the risk of this high profile threat, so that you can avoid the business disruption, loss of productivity, damage to brand reputation and legal implications that come along with recovering from a ransomware attack.

DEFEATING RANSOMWARE WITH TREND MICRO

There is no silver bullet when it comes to ransomware; it requires a multi-layered, step-by-step approach for the best risk mitigation.



Email and web protection

Endpoint protection

Network protection

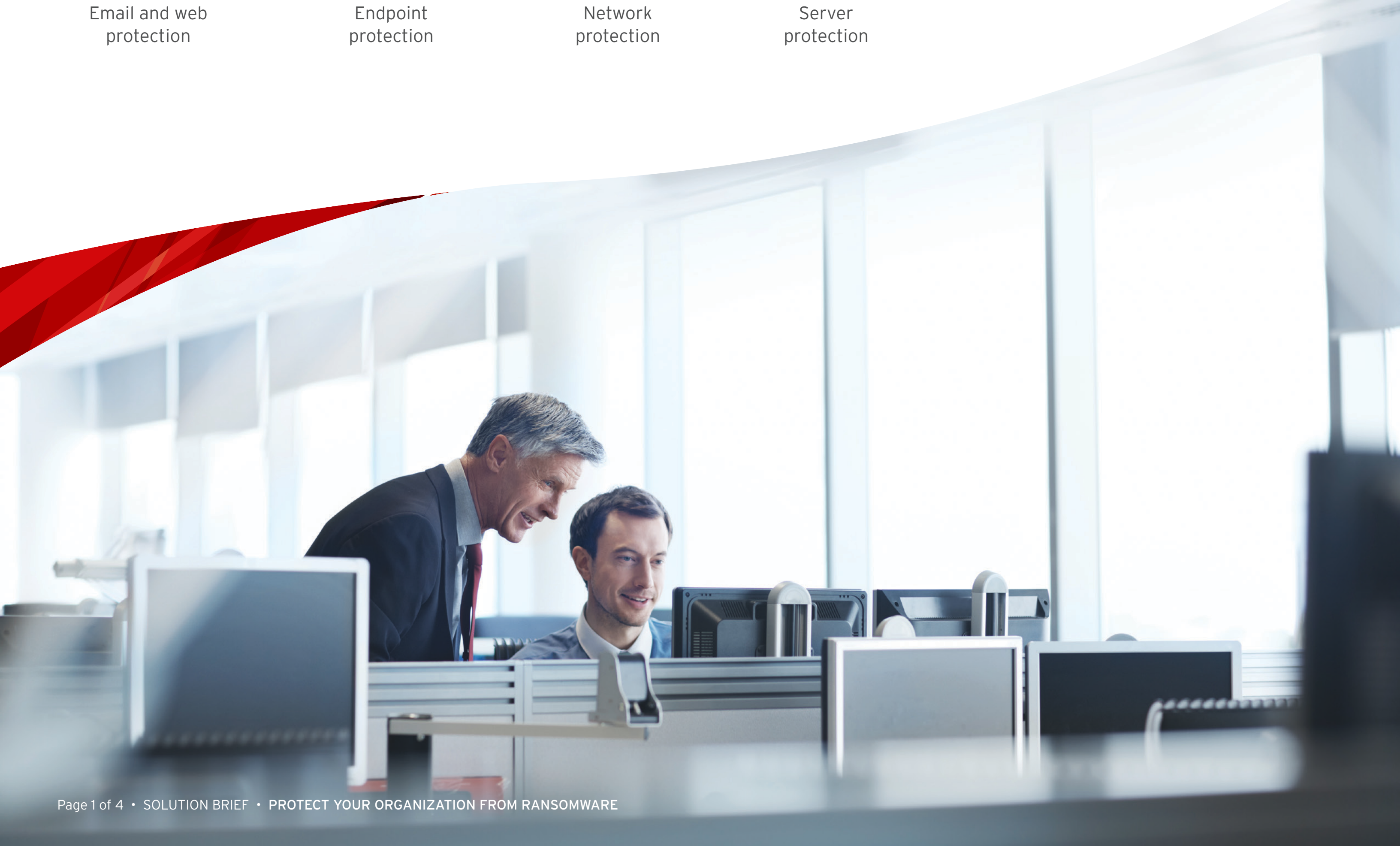
Server protection

What is ransomware?

Ransomware is a type of malware that locks, encrypts, or otherwise prevents data and systems from being accessed by their owners, and requires victims to pay a ransom to the criminal responsible for the attack in order to regain access.

It is primarily distributed via exploit kits, social engineering schemes and spam mails that are sent to a large number of email addresses. When a recipient opens a malicious attachment or clicks a compromised link, the malware is downloaded on to the user's system.

The fear of losing priceless data can push users to pay the ransom—and while they may opt to pay, having their files unlocked or decrypted is never a guarantee.



EMAIL AND WEB PROTECTION

It all starts with your users. They're the most vulnerable when it comes to ransomware – whether it's falling for a phishing email or clicking on a malicious URL, users are the easiest target for attackers. Trend Micro has blocked over 99 million ransomware threats since October 2015, and 99 percent of those were found in malicious emails or web links[1]. By blocking ransomware at the email and web gateway, you can prevent it from ever reaching your users.

Using Microsoft Office 365 for Email?

Even though you are relying on a cloud-based email solution with built-in security, you are still highly vulnerable to ransomware attacks via phishing emails or malicious attachments. That's where Trend Micro can help. **Trend Micro Cloud App Security** has blocked more than 2 million threats that weren't detected by the built-in Office 365 security, augmenting built-in security to detect ransomware with:

- Malware scanning and file risk assessment
- Sandbox malware analysis
- Document exploit detection
- Web reputation

Relying on an Email Gateway for on-premises Email Protection?

Improve your email gateway ransomware detection rates. **Trend Micro™ Deep Discovery™ Email Inspector** uses advanced detection techniques to identify and block spear phishing emails that are often used to deliver ransomware to unsuspecting employees. By working seamlessly, and in tandem, with your existing email gateway or server security products, Email Inspector can detect and block purpose-built spear phishing emails, which use malicious attachments and URLs as common delivery vehicles for ransomware. Email Inspector delivers:

- In-depth analysis of email attachments and URLs, including: Office Docs (+macros), PDFs, archives, executables, scripts, multimedia, and more
- In-depth virtual analysis of URLs, including: URLs embedded in body or subject of messages and URLs embedded within documents
- Script emulation and zero-day exploit detection to detect ransomware and related activity, including: mass file modifications, encryption behavior and other modifications

Minimizing the Risk from Web Traffic

Beyond email, your users are susceptible to ransomware by clicking on web sites that are either intentionally malicious, or have been compromised. **Trend Micro™ InterScan™ Web Security** protects your users on the web with:

- Scanning for zero-day exploits and browser exploits, which are common paths ransomware uses to enter your organization
- Integration with Trend Micro™ Deep Discovery™ for sandbox analysis
- Real-time web reputation to determine if a URL is a known delivery vehicle for ransomware

Known Ransomware Threats

PowerWare – This malware has the ability to enumerate all logical drives, including drives mapped to shared networks. This puts an entire network at risk and could be a major threat to enterprises.

PETYA – Can overwrite an affected system's master boot record to lock users out. Infected units receive the ransom note when they boot up the system and can't go any further. It is delivered to victims via legitimate cloud storage services.

KeRanger – An encryption malware that is the first crypto-ransomware for Mac and is installed via an open source file-sharing application. Creators of the malware used a Mac app developed certificate to get past Apple Gatekeeper, a security feature that allows users to restrict which sources they can install apps from.

SAMAS (also known as SAMSAM) -The first ransomware that has the ability to encrypt files across networks, threatening an organization's database and network-stored backups. Users of SAMAS are known to manually locate and delete network backups to force companies to pay ransom.

Locky - searches and deletes Volume Shadow Copy of files, which are automatic backup files for Windows.

MAKTUBLOCKER – The encryption method of this ransomware is similar to most, its infection vector is unique. It comes in the form of an email that has the user's name and mailing address, making the email seem trustworthy. When they download the attached file, the ransomware is activated.

[1] Trend Labs, April 2016

ENDPOINT PROTECTION

Trend Micro detected 99 percent of ransomware threats in email messages or web links. That still leaves 1 percent that could make it through to your endpoint. Trend Micro Smart Protection Suites deliver several capabilities that minimize the risk of ransomware to your endpoints, including:

- **Behavior Monitoring:** for suspicious behavior associated with ransomware, such as the rapid encryption of multiple files, so that the encryption process can be automatically stopped and the endpoint isolated, before the ransomware can spread and cause more damage to your data.
- **Application Control:** dynamically and automatically creates application white lists, which will only allow known good applications to execute, and prevent the execution of unknown applications such as ransomware.
- **Vulnerability Shielding:** protects you from ransomware that takes advantage of unpatched software vulnerabilities, a target for exploit kits in attacks. This includes shielding end-of-support systems like Windows XP.

NETWORK PROTECTION

Email and web are common ways ransomware enters your organization, but other network protocols and attack methods can expose you to ransomware. That's why you need a network defense strategy that stops ransomware from accessing and spreading within your network.

Trend Micro™ Deep Discovery™ Inspector is a network appliance that detects malicious traffic, command and control communications, attacker behavior, zero-day exploits and other activity that is associated with attempts to infiltrate ransomware into and across your network. Deep Discovery can prevent ransomware from spreading to other endpoints and servers. It protects against ransomware with:

- Extensive detection techniques across all network traffic, ports and over 100 network protocols to identify ransomware and attacker behavior across the entire kill chain
- Proven sandbox analysis that mirrors your computing environment to detect file modifications, encryption, and malicious behavior that is consistent with ransomware attacks
- Integration with Trend Micro email and web gateways, and endpoint, server protection, and third party solutions to provide a connected threat defense where new threat information is shared across multiple layers

Protect your organization from Ransomware

- Leverage automated back-up and restore processes
- Apply software patches as soon as they become available
- Educate employees on on prevention of email phishing
- Limit access to business critical information
- Bolster your security posture with layered ransomware protection

SERVER PROTECTION

Ransomware is increasingly targeting servers, including recent high profile examples like SAMSAM, where attackers are targeting known software vulnerabilities to inject ransomware. Attacks on your servers, where the majority of your critical data resides can be particularly disruptive to your business.

Trend Micro™ Deep Security™ protects your servers across the hybrid cloud (physical, virtual and cloud) from ransomware with:

- **Suspicious Activity Detection and Prevention:** If ransomware attempts to gain a foothold in a data center (e.g. via a compromised user connecting to a file server), Deep Security can detect suspicious network activity and prevent it from continuing, while also alerting that there is an issue.
- **Vulnerability Shielding:** Protects servers and applications from ransomware attacks by shielding them against exploits of known software vulnerabilities that could be used to inject ransomware, including in end-of-support systems like Windows 2003.
- **Lateral Movement Detection:** If ransomware should get into the data center, Deep Security can also help to minimize the impact by detecting and blocking it from spreading to more servers.

When ransomware infects your organization, it can access whatever data a compromised user in your organization can access. It can consume several man hours as your organization tries to recover lost files through email threads, with little hope of recovery.

As ransomware evolves, organizations need to keep up with the threat. Partner with Trend Micro and get solutions that prevent and mitigate the damages caused by this potentially devastating threat.

For more information, visit
trendmicro.com/enterprise-ransomware

ABOUT TREND MICRO

As a global leader in cloud security, Trend Micro develops security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, Trend Micro delivers top-ranked security that fits customers' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

TREND MICRO™

Securing Your Journey to the Cloud