proofpoint.

SOLUTION BRIEF

How Proofpoint Defends Against Ransomware

Stop ransomware from taking root and spreading in your organization

Products

- Proofpoint Threat Protection
- Proofpoint Cloud Security

Key Benefits

- Prevent initial infection
- Prevent discovery, lateral movement and persistence
- Prevent data exfiltration

Ransomware is one of today's most disruptive forms of cyber attack. It puts victims out of business, forces hospitals to turn away patients and brings entire governments to a standstill. It has evolved into one of the most menacing cyber threats today. Last year alone, the United States experienced more than 65,000 ransomware attacks. The threat is a top concern for CISOs and it has become a national security issue. Most alarmingly, many organizations are wholly unprepared for a ransomware attack. Just 13% of IT experts surveyed by the Ponemon Institute said their company can prevent ransomware. And more than 68% consider themselves "vulnerable" or "very vulnerable."[1]

Email and web are the primary ransomware attack vectors. Most ransomware attacks today are multistage. With these attacks, email or compromised websites play an integral part in the initial stages of the attack chain. They often deliver an initial payload as a malware downloader. These payloads are designed to gain entry into a user's system. And they are often used to steal credentials and gain access to the user's network. Ransomware actors also use stolen credentials to gain access to internet-exposed services. Common tactics include credential phishing emails, brute forcing passwords and drive-by compromises.

Once initial access has been gained, ransomware actors establish persistence, conduct reconnaissance and move laterally. Inside, attackers not only can encrypt sensitive files, but they can also exfiltrate sensitive information for double-extortion tactics.

As backup and recovery measures have become more successful at thwarting ransomware attacks, threat actor tactics have evolved to overcome them. Ransomware actors are now using what's called double-extortion ransomware. This tactic first exfiltrates sensitive data, then it encrypts the files. If the victim

1 The Ponemon Institute. "The Rise of Ransomware." January 2017.

organization refuses to pay to have the files decrypted, then the threat actor has three avenues to demand payment:

- Threaten the victim to leak the data online
- Sell it to the highest bidder
- Send direct emails to the victim's customers and partners threatening to leak their data

Because email is the initial infection point for most ransomware attacks, a large percentage of ransomware starts, directly or indirectly, with a phishing email. These emails trick users into opening a malicious attachment or clicking a malicious URL. You need advanced solutions to detect and block such threats from compromising a user's credentials. As more of your organization's data is stored in the cloud, so too are password files and sensitive data. Limiting data exposure in the cloud is important to help minimize what is shared with threat actors.

Proofpoint sees ransomware attacks becoming more targeted, more damaging and increasingly disruptive to business operations. Proofpoint Threat Protection and Proofpoint Cloud Security can help prevent them. Our comprehensive, integrated platforms reduce the risk of ransomware attacks by layering controls that:

- Prevent the initial infection
- Detect initial access and prevent discovery, lateral movement and persistence
- Prevent data exfiltration

Prevent the Initial Infection

Proofpoint Threat Protection and Proofpoint Cloud Security prevent initial infections by:

- Detecting and blocking ransomware and malware downloaders that lead to ransomware
- Preventing credential compromise
- Providing visibility into ransomware risks
- Isolating URL clicks based on risk
- Training users to identify and report malicious messages
- Automating remediation of email threats

Detect and block ransomware and malware downloaders

The Proofpoint Threat Protection platform detects and blocks ransomware as the initial payload. It also blocks malware that leads to ransomware. We provide multiple machine learning-based engines to detect malware, malicious code and evasion detection techniques. This protects users from malicious websites or ransomware-infected files.

The platform conducts reputation and content analysis. It also runs sandboxes for in-depth analysis of URL- and attachment-based threats. We employ predictive analysis that identifies and sandboxes suspicious URLs based on changes in attacker tactics. For example, because attackers often use legitimate file-sharing sites to host malware, the platform sandboxes all file-sharing URLs. Solutions that rely only on reputation analysis would miss these attacks.

Prevent credential compromise

Attackers use different tactics to steal a user's credentials. Some methods include phishing, brute force attacks, dark web and exposed information stored in a user's cloud storage. Once an attacker has access to your credentials, there is no need to send a downloader anymore. They can simply log on to your VPN or sign into internet-facing services using your credentials. From there they can steal confidential data or encrypt files. As organizations adopt additional cloud services, negligent users may upload password files and sensitive data to the cloud.

Proofpoint Threat Protection detects and stops phishing messages using multiple detection engines, including machine learning classifiers that inspect URLs. Proofpoint Cloud Security can identify sensitive information exposed in cloud accounts that attackers could exploit.

Figure 1: Three layers of protection.

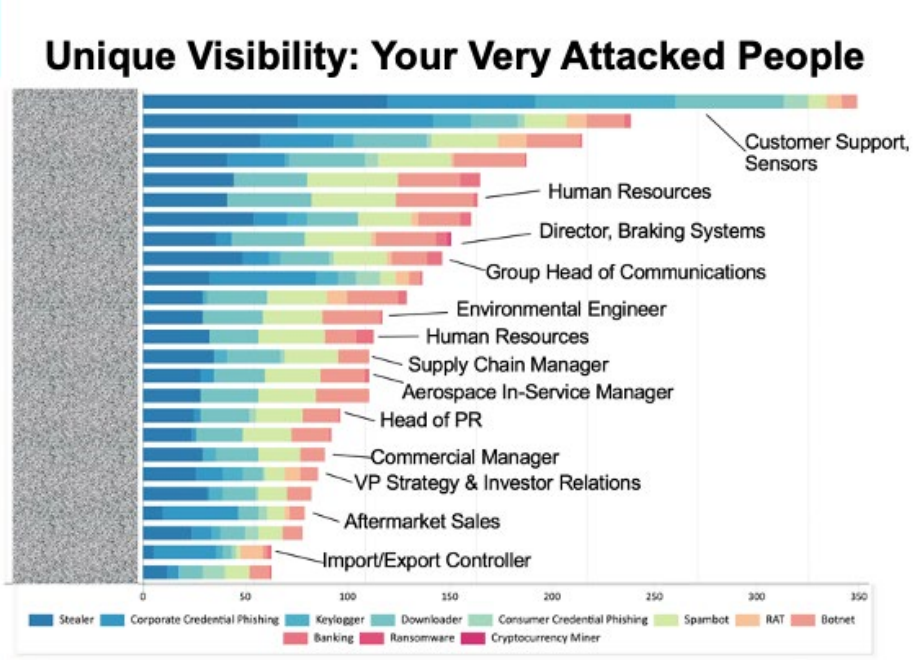

Figure 2: Proofpoint provides visibility into your Very Attack People (VAP).

Get visibility into your ransomware risk

Proofpoint provides visibility into your Very Attacked People™ (VAP). VAPs are the people in your company most exposed to attacks. This visibility highlights who is most targeted and what threats are targeting them. The data lets you adjust your defense strategy to the specific threats that your VAPs face.

Proofpoint also provides detailed information on threats and campaigns. The threat insight dashboard shows in-depth forensics. Data includes threat actor, spread, message samples, intended recipient, attack progression and more.

Reduce impact with integrated email isolation

Attackers can weaponize URLs post-delivery. This strategy helps them evade initial detection. But Proofpoint Browser Isolation reduces the impact of users clicking on malicious URLs. It provides time-of-click protection for URLs within corporate emails. And it isolates browsing activity in a secure container that displays only a safe-rendered version to users. It also prevents first-stage downloaders and credential theft. This essentially breaks the attack chain.

You can implement risk-based isolation based on policy and with our VAP insights. You can send the riskiest URLs into isolated browsing sessions. You can also set stricter policies for targeted people by isolating all user clicks. Depending on which users are being targeted, we can also adapt the isolation policy based on the riskiness of the user and the riskiness of the URL they click on.

Make your users security aware

Ransomware prevention requires that you train your people. After all, your users are your last line of defense. Ransomware attacks require a user to click a link or download an attachment. According to the latest 2021 Verizon DBIR report, 85% of breaches last year involved a human element.[2]

The Threat Protection platform includes security awareness training. This training lets you educate your users about ransomware and train them to not click on suspicious messages. You can assign more training to those users who are most targeted and those who have actually interacted with real threats. To further cement end-user training, you can use content from our vast content library in your employee communications and security alerts. You can also run simulated attacks using templates based on real-life lures seen across the billions of messages that Proofpoint analyzes. The platform provides easy mechanisms to report suspicious emails via our PhishAlarm button and email warning tags.

2 Verizon. "DBIR: Data Breach Incident Report." 2021.

Users' account credentials are the keys to your kingdom. With just a single username and password a ransomware operator can launch attacks inside and outside of your organization.

Automate remediation of malicious messages

Security teams are often understaffed. And they are often overwhelmed with alerts that need to be quickly triaged and investigated. The Threat Protection platform provides email-focused security orchestration automation and response (mSOAR). It automates the investigation and remediation of user-reported and malicious or unwanted email.

User-reported messages are automatically analyzed and enriched using multiple threat intelligence and reputation systems. If the message is malicious, it and any related messages can be quarantined automatically. It cuts the need to investigate each alert and remediate malicious messages manually. Your security team thus saves a lot of time and effort. To close the loop, the users get a customized email confirming that the message was malicious. This serves to reinforce good behavior.

The Threat Protection platform analyzes messages even post-delivery. If the platform sees that something is malicious after delivery, it will trigger an automatic pull from the user inbox. It will even pull messages that have been forwarded to other users or sent via distribution lists.

Detect Initial Access and Prevent Discovery, Lateral Movement and Persistence

Proofpoint Cloud Security detects ransomware threats by:

- Monitoring and detecting compromised cloud accounts
- Monitoring for malicious file uploads to cloud accounts
- Protecting from command and control with web security
- Limiting network access with zero-trust access controls

Detect cloud account takeover

Users' account credentials are the keys to your kingdom. With just a single username and password—especially for cloud apps such as Office 365 or Google Workplace—a ransomware operator can launch attacks inside and outside of your organization. Proofpoint Cloud Security's CASB provides real-time adaptive access controls. These are based on risk, context and role. It automatically blocks access to cloud apps from risky locations and from known threat actors. CASB also uses contextual data to confirm a user's identity and prevent risky access. Contextual data includes user location, device, network and log-in time. You can define access policy controls such as enforcing multifactor authentication and restricting access from unmanaged devices to protect from ransomware actors.

Proofpoint gives you the visibility to surface the lateral spread or risk to your data because of a compromised account. You can see if a suspicious login is correlated to an account that sends malicious emails. It lets you see if a threat actor tried to install persistent access through setting email forwarding and delegation rules or by using OAuth tokens. It also lets you know what suspicious file activity occurred.

Prevent ransomware distribution from cloud apps

Ransomware can spread through the sharing of infected files and automatic syncing. It has the potential to severely impact your organization, partners and customers. Proofpoint Cloud Security actively monitors your cloud file shares and alerts you when there is a suspected file. With Proofpoint sandboxing and analytics of files in cloud apps, you can contain those malicious files in the cloud through an automated quarantine and other mitigation steps.

Protect from command-and-control with web security

Once a device is compromised, it sends a signal to the threat actor's servers. The actor then looks for the next set of instructions. With control of the device, the ransomware actor can perform a range of actions. These actions range from distributing ransomware to exfiltrating data.

Proofpoint Cloud Security's Web Security and Browser Isolation blocks connections to compromised sites. It thus prevents the ransomware operator from being able to control the device and cause further damage. The intelligence is powered by Proofpoint Nexus Threat Graph. This combines trillions of real-time data points across multiple threat vectors around the world, advanced AI and machine learning and a global research team that keeps you ahead of today's biggest cyber threats.

Limit the ransomware blast radius with zero trust network access controls

Ransomware operators also exploit legacy VPNs to launch their ransomware attacks. Once a VPN is compromised, the threat actors have broad access. This makes it easy for them to move laterally across the full network. Lateral movement means greater surface area for the ransomware actor to probe for ransom-worthy data. The more interesting the data, the higher the ransom.

Proofpoint Cloud Security Zero Trust Network Access (ZTNA) limits the visibility of ransomware actors by providing users with microsegmented secure access to help identify and remediate over-permissioned and/or sensitive files. Users are only granted access to the applications they need, not the full network. For threat actors, less access means less data to steal, encrypt and destroy. This translates to less ransom to demand—you can't attack what you can't see. So, you've effectively made the crime harder to commit.

Prevent Data Exfiltration

Proofpoint Threat Protection and Proofpoint Cloud Security prevent data exfiltration by:

- Watching for early signs of data exfiltration
- Detecting and preventing unauthorized data movement

Proofpoint Cloud Security's Web Security and Browser Isolation delivers risk-aware data security that can perform data loss prevention (DLP) in real time. Together with Browser Isolation, Web Security provides granular data controls like read-only access and allowing or blocking for cloud apps and web. Browser Isolation secures users' access to apps and data by isolating browser sessions in a secure container.

In addition, Proofpoint CASB helps you gain visibility quickly to suspicious file activity. Notably, it is linked to suspicious logins. Responders can quickly separate attacker-initiated file activity from user-initiated file activity. And with this ability, they can respond in a timely fashion.

Beyond protecting sensitive data in cloud apps, Proofpoint can block sensitive content from being exfiltrated via command and control, downloaded to unmanaged (ransomware operator's) devices, and from being emailed out.

LEARN MORE

For more information, visit **proofpoint.com**.