Surviving Ransomware–What You Need to Know

Ransomware has a longer history than many realize, with its roots going back to the 1980s. The first recorded ransomware attack occurred in 1989 with the AIDS Trojan, distributed via floppy disk at the World Health Organization's AIDS Conference—also marking it as one of the earliest instances of major hacktivism.

However, ransomware's evolution accelerated in the 2000s. In 2006, the Archievus virus emerged as the first ransomware to use advanced RSA encryption, leveraging websites and spam email for mass distribution. This marked a significant technological leap, though a uniform decryption password limited its impact. By 2008, the arrival of bitcoin—officially launching in January 2009—provided a game-changing ability to make it harder to trace transactions and fueling ransomware's rapid growth.

More recent attacks include high-profile ransomware groups like LockBit and Clop, both of which have made headlines with increasingly sophisticated tactics. LockBit, known for its ransomware-as-a-service (RaaS) model, has carried out numerous attacks targeting critical infrastructure, healthcare, and financial sectors, evolving its tactics with fast encryption speeds and double-extortion schemes. Clop, another major player, is notorious for exploiting zero-day vulnerabilities in file transfer software, such as MOVEit, leading to massive data breaches across global enterprises. These groups exemplify how malicious actors are continually refining their techniques, from exfiltrating data for leverage to attacking supply chains, leaving security practitioners facing increasingly formidable and adaptive threats.

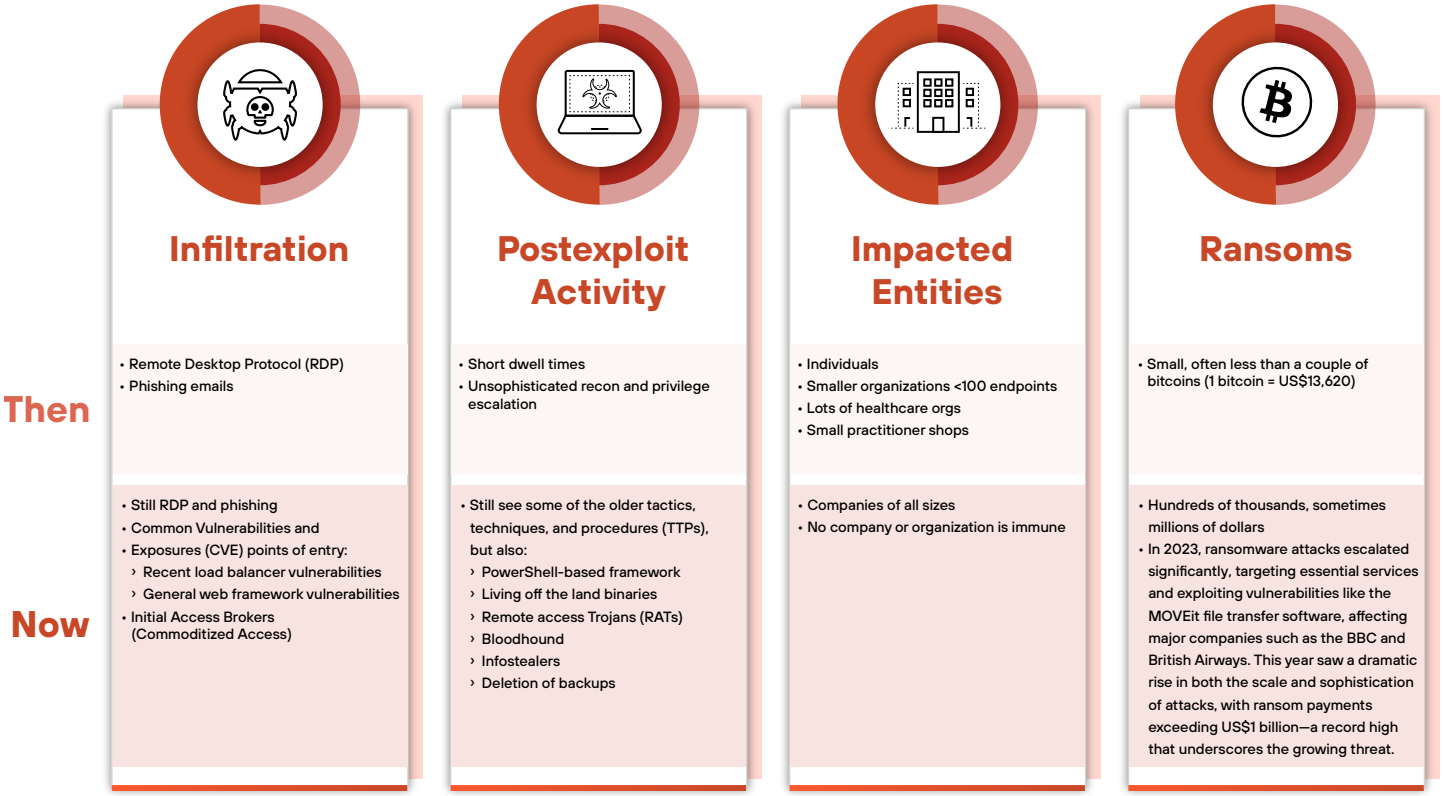

Figure 1: Ransomware: then and now

Ransomware 101: The Basics

Ransomware is a criminal business model that uses malicious software to hold data hostage, often locking and/or encrypting a system while demanding a ransom payment in exchange for restoring access. While an increasingly urgent challenge, you can prevent ransomware. Or at least, you can minimize damage through proper training, specific tunings in your current IT environment, and deploying advanced endpoint technology. This technology deployment includes adding solutions such as eXtended detection and response (XDR) to your security stack.

Ransomware can be divided into two basic types:

- *Crypto ransomware*, the most common, which encrypts files and data.
- *Locker ransomware*, which locks the computer or other device, preventing the victims from using it.

Crypto ransomware encrypts the data, so even if the malware is removed from the device or the storage media is moved to another device, the data isn't accessible. Typically, crypto ransomware doesn't target critical system files, enabling the device to continue to function despite being infected. After all, the device could be needed to pay the ransom.[1]

Locker ransomware only locks the device, while the data stored on the device is typically untouched. As a result, if the malware is removed, the data is untouched. Even if the malware can't be easily removed, you can often recover the data by moving the storage device (typically a hard drive) to another functioning computer.

Most ransomware attacks consist of the following steps unless the attack is mitigated or the victim refuses to pay the ransom:

1. **Compromise and Take Control of a System**

   Most attacks begin with phishing, tricking a user with a fraudulent email to open an infected attachment that compromises the system, or they may include other forms of valid credential abuse for initial access. This may impact a single host, such as a computer or mobile device. Then the compromised host will establish communications to a command-and-control (C2) server. The attacker might, at that point, move laterally from the initial host to other systems in the organization to maximize the impact of the ransomware attack.

2. **Discover or Exfiltrate Valuable Data**

   While ransomware in the past would often simply identify and encrypt certain file types likely to be of value to the victim (e.g., business documents like .doc, .xls, and .pdf), attackers have evolved. Now, it's more common for threat actors to silently seek out known sensitive data, including customer data or intellectual property data, to ensure they can command higher ransoms. Attackers also often exfiltrate data for use in multiextortion schemes, detailed below.

3. **Prevent Access to the System**

   Once an attacker infects the system, they either encrypt data or deny access to a system or multiple systems through lockout screens or scare tactics.

4. **Alert the Owner of the Device About the Compromise, Ransom Amount, and Steps They Should Take**

   As you'll notice, all of the previous steps are the actual bulk of the ransomware attack, and, if performed by a skilled adversary, they'll be performed without the victim knowing. This means, when the attacker notifies victims of their presence, the attack is done. This notification often comes in the form of a ransom note with payment instructions and additional steps to unlock their devices.

5. **Accept Ransom Payment**

   An attacker must have a way to receive ransom payments while evading law enforcement, which explains the use of pseudoanonymous cryptocurrencies such as bitcoin for these transactions.

6. **Promise to Return Full Access Upon Payment Receipt**

   Failure to restore compromised systems will destroy the scheme's effectiveness, as no one pays a ransom without confidence that their valuables will be returned.

1. Ronny Richardson and Max M. North, "Ransomware: Evolution, Mitigation and Prevention," Kennesaw State University, January 1, 2017.

Common Attack Methods

To better prevent ransomware, it's critical to understand the tactics attackers use to deliver this threat. There are multiple ransomware families that threat actors use, across multiple attack vectors. These vectors include coming through the network, software-as-a-service (SaaS) applications, and directly to the endpoint. This information will enable you to focus your security controls on the areas most likely to be leveraged and reduce the risk of infection.

Increasingly, artificial intelligence is being leveraged to create more convincing phishing emails and social engineering attempts. AI-generated text can mimic legitimate communication styles, making malicious emails harder to distinguish from genuine ones. This evolution in attack sophistication necessitates more advanced detection methods and user education.

Malicious Email Attachments

Historically, with malicious email attachments, the attacker would craft an email. This message is likely to come from a believable source such as human resources or IT and attach a malicious file such as a Portable Executable (PE) file, a Word document, or a JS file.

The recipient opens the attachment thinking the email has been sent from a trusted source. Once the file is opened, the ransomware payload is unknowingly downloaded, the system is infected, and the files are held for ransom. Today, malware infections often give access to attackers who will later deploy ransomware.

Malicious Email Links

Similar to malicious email attachments, malicious email links are URLs in the body of the email. Likewise, these emails are sent from someone or some organization that you believe to be a trusted source. When clicked, these URLs download malicious files over the web, the system is infected, and the files are held for ransom.

Vulnerable Credentials

Ransomware operators may also buy credentials from initial access brokers (IABs) or take advantage of poor password hygiene to avoid the whole process of actually compromising the victim. IABs are individuals who gather and collect credentials, selling them to the highest bidder.

While IABs aren't exclusively for ransomware, ransomware operators definitely leverage the system, typically at the beginning of the intrusion lifecycle. IABs are used to conduct reconnaissance, identifying networks with vulnerable applications or devices such as virtual private networks (VPNs), open RDP, or servers with exposed software vulnerabilities. With solid best practices such as multifactor authentication (MFA) and additional identification mechanisms, you can avoid this vector.

Are You at Risk?

One might assume only large corporations are the targets of ransomware. That said, small businesses aren't immune to compromise. The Verizon 2023 Data Breach Investigations Report, released in 2023, found that small businesses continue to be significant targets for cyberattacks, including ransomware, noting that 43% of cyberattacks target small businesses.[2]

Ransomware attacks can have a very public impact, as victim organization operations may be severely degraded or shut down entirely, as illustrated by recent attacks on hospitals across the United States. Personally identifiable information (PII) can be a veritable goldmine of data for cyberthieves who can sell or auction it off on the dark web. The exposure of PII may lead to more identity fraud and targeted scams that may impact consumers.

2. *2023 Data Breach Investigation Report*, Verizon Business, June 6, 2023.

Criminals have realized that this is a lucrative business with low barriers to entry. As a case in point, the ransomware-as-a-service model allows affiliates to use already-developed ransomware tools to execute ransomware attacks.

Consequently, ransomware is displacing other cybercrime business models. Moreover, attackers are becoming increasingly sophisticated in their ability to determine the value of compromised information, assess the victim organization's willingness to pay, and demand higher ransoms.

More Platforms Are Vulnerable

While attackers focused almost exclusively on Microsoft Windows systems in the past, the emergence of ransomware for Android, macOS, and now Linux demonstrates that no one operating system is immune to these attacks. Nearly all computers or devices with an internet connection are potential victims of ransomware, which is a valid concern with the proliferation of IoT devices and, most recently, an expanded attack surface due to a surge in remote workers.

Supply Chains and Critical Vulnerabilities in the Crosshairs

In 2023, the ransomware landscape experienced significant transformations, with supply chain attacks and exploitation of critical vulnerabilities playing a central role in the surge of ransomware activity.

The year saw a 49% increase in victims reported by ransomware leak sites, with a total of 3,998 posts from various ransomware groups.[3] This dramatic rise can be largely attributed to the exploitation of critical vulnerabilities in widely used software and services.

Key Findings from 2023 Attacks[4]

1. **Critical vulnerabilities exploited**: Zero-day exploits targeting vulnerabilities like CVE-2023-34362 for MOVEit Transfer and CVE-2023-4966 (Citrix Bleed) drove spikes in ransomware infections before defenders could update the vulnerable software.
2. **Supply chain impact**: The CL0P ransomware group's exploitation of the MOVEit vulnerability alone affected an estimated 2,730 organizations, highlighting the cascading effect of supply chain attacks.
3. **Emerging threats**: At least 25 new ransomware groups emerged in 2023, indicating the continued attraction of ransomware as a profitable criminal activity.
4. **Industry focus**: Manufacturing was the most affected industry in 2023, accounting for 14% of ransomware leak site posts. This sector's reliance on complex supply chains and operational technology (OT) systems makes it particularly vulnerable.
5. **Geographic distribution**: While ransomware affected organizations in at least 120 countries, the US remained the primary target, accounting for 47.6% of ransomware leak site posts in 2023.

3. Doel Santos, *Ransomware Retrospective 2024: Unit 42 Leak Site Analysis*, February 5, 2024.
4. 2023 Unit 42 Ransomware and Extortion Report, Palo Alto Networks, March 21, 2023.

Evolution of Tactics

Ransomware groups have adapted their tactics to maximize impact and profits:

- **Multistage attacks**: Some groups use ransomware as a distraction or funding source for more complex supply chain compromises.
- **Data exfiltration**: Groups like CL0P updated their tactics to use torrents for distributing stolen data, increasing efficiency in their extortion efforts.
- **Targeting critical infrastructure**: Ransomware operators increased their focus on sectors with low tolerance for downtime, such as manufacturing and healthcare.

Law Enforcement and Cybersecurity Response

2023 saw intensified efforts from international law enforcement agencies, leading to the decline of groups like Hive and Ragnar Locker, and the near-collapse of ALPHV (BlackCat). These actions reflect the increasing challenges faced by ransomware groups and the growing effectiveness of global cooperation in cybersecurity.

Future Trends and Predictions

Looking ahead, Unit 42 (Palo Alto Networks threat intelligence and consulting arm) experts predict several developments that could impact supply chain security:

- A potential large-scale cloud ransomware compromise, which could have far-reaching effects on cloud-based supply chains.
- An increase in extortion related to insider threats, which could facilitate supply chain attacks.
- A rise in politically motivated extortion attempts, potentially targeting critical supply chains.
- The use of ransomware and extortion to distract from attacks aimed at infecting supply chains or source code.

As supply chain attacks continue to evolve, organizations must adapt their defenses to address not only the technical aspects of these threats, but also the potential for reputational damage. They also need to protect employees, customers, and partners who may become targets in these increasingly complex attacks.

Harassment has emerged as another prominent extortion tactic. Ransomware groups now frequently target specific individuals within an organization, often focusing on C-suite executives with threats and unwanted communications. By late 2022, harassment was a factor in about 20% of ransomware cases, a stark increase from mid-2021 when it was present in less than 1% of cases.[5]

5. *2024 Unit 42 Incident Response Report*, Palo Alto Networks, February 20, 2024.

The Four Pillars of Multiextortion

Ransomware operators are increasingly employing multiple extortion techniques to pressure victims into paying. This trend of multiextortion has evolved significantly since 2021, with threat actors layering various tactics to maximize their chances of a payout.

The rise of quadruple extortion (figure 1) is one disturbing trend identified by Unit 42® back in 2021. Ransomware operators now commonly use as many as four techniques for pressuring victims into paying:

- **Encryption**: Victims pay to regain access to scrambled data and compromised computer systems.
- **Data theft**: Hackers threaten to release sensitive information if a victim doesn't pay the ransom.
- **Denial of service (DoS)**: Ransomware gangs launch DoS attacks that shut down a victim's public websites.
- **Harassment**: Cybercriminals contact customers, business partners, employees, and media to inform them of the hack and increase pressure on the victim organization.

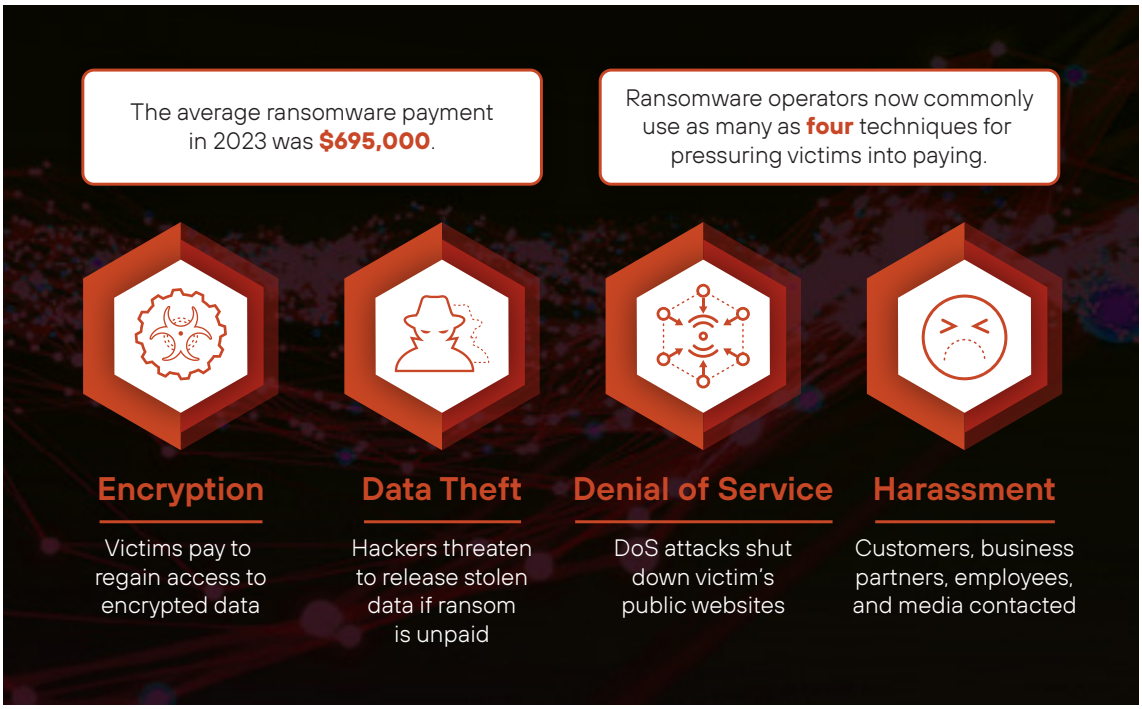

Figure 2: Quadruple extortion is on the rise

While it's rare for one organization to fall victim to all four techniques, the trend shows that attackers are increasingly willing to use multiple methods to achieve their goals.

And as they've adopted these new extortion approaches, ransomware gangs have remained greedy. Among the dozens of cases that Unit 42 consultants reviewed in 2023, the median ransom demand was $695K.[6]

The ransomware crisis will continue to gain momentum over the coming months as cybercrime groups further hone tactics for coercing victims into paying and developing new approaches for making attacks more disruptive.

6. *2024 Unit 42 Incident Response Report*, Palo Alto Networks, February 20, 2024.

Extortion Without Encryption on the Rise

As a departure from past tactics, about 10% of Unit 42's incident response matters involving extortion didn't involve encryption.[7] These cases often rely on data theft alone, with some threat actors even deleting organizations' data altogether instead of encrypting it.

As ransomware groups continue to evolve their tactics, organizations must adapt their defenses to address these various methods of applying pressure. Modern incident response plans need to consider not only technical aspects but also safeguards for an organization's reputation. They must also include measures to protect employees, customers, and partners who may become targets of increasingly aggressive extortion tactics.

Prepare and Prevent

Ransomware acts quickly—sometimes within minutes of infection—so it's critical to take action and deploy controls that either mitigate or prevent ransomware attacks. The next two sections summarize the top recommendations to do both.

Recommendations to Mitigate the Impact of a Ransomware Attack

Develop and execute a plan for an end-user awareness program.

- It can be difficult to get approval to send regular company-wide security reminders but smarter end users who are more aware of cybersecurity risks will surely experience fewer ransomware incidents.

Review/validate server backup processes.

- Backups that are configured improperly or in a location that can allow for further compromise can result in further losses, both monetary and otherwise.
- Review critical file servers that host network shares for critical departments and plan for regular review of the recovery process for these servers.

Conduct end-user privilege reviews.

- Assign a trusted delegate to develop and organize a process to evaluate permissions that users have on mapped network drives. Whenever possible, implement the principle of least privilege to minimize the impact that any single user can have.
- Start the review process by looking at end-user privileges for critical resources and departments.
- Require strong, unique, and complex passwords for all accounts.
- Review network drive permissions to minimize the impact a single user can have.

Define administrator user privilege reviews.

- Audit privileged roles used by the server, backup, and network teams to validate appropriate access.
- Ensure administrators are assigned normal, restricted accounts, separate from their highly privileged accounts.
- Require administrators to use their highly privileged accounts only when they need them.
- Remove automatic network drive mappings from administrative accounts, where possible.
- Restrict administrative accounts from receiving email.
- Require MFA for all users, including administrative accounts, and monitor for abnormal use.
- Require strong, unique, and complex passwords for all accounts.

7. *2023 Unit 42 Ransomware and Extortion Report*, Palo Alto Networks, March 21, 2023.

Document your incident response plan for ransomware.

- Ensure ransomware response processes are included in your incident response plan. Ransomware requires a unique process to recover and should stand out on its own.
- Cases where all the files on an entire department drive are encrypted can become quite complex as multiple teams need to be engaged—backup team, file-server team, endpoint, directory team, and others. The more you plan now, the quicker your response time will be.

Top Recommendations to Prevent Ransomware Infections

Promptly apply software patches.

- Review your patching processes and risk acceptance and look for opportunities to remove roadblocks.
- Ensure VPN and file sharing services are up to date.

Protect against email-based threats.

- Configure protections for inbound mail and block files most likely to present a higher risk.
- Prevent users from enabling macros by blocking macros from running in Microsoft applications. That said, many organizations implement policies and technical controls to restrict macro execution across all applications, not just Microsoft products. This is often done through endpoint protection platforms, group policies, or application control software.
- Inspect emails for malicious URLs.
- Train end users on phishing and social engineering techniques.

Deploy a next-generation firewall.

- Ensure your firewall automatically blocks known threats based on a trusted threat feed that constantly updates.
- Ensure your firewall provides sandboxing capabilities so you can stop unknown threats (URLs and executables) before they reach the endpoint.
- Configure your firewall/proxy to require user interaction for end users communicating with websites labeled as "uncategorized" (e.g., click a "Proceed" button). Attackers use many uncategorized websites in targeted phishing campaigns to distribute malware. This two-step process prevents certain types of ransomware from making that external call to the C2 server. If that doesn't happen, your files may not be encrypted.
- Ensure signatures are up to date regarding remote desktop vulnerabilities.
- Ensure your next-generation firewall includes advanced URL filtering capabilities to detect unknown threats.

Deploy advanced endpoint protection.

- Ensure that your endpoint protection measures can detect and prevent known and unknown malware, as well as known and unknown exploits, including zero-day exploits.
- Add behavior-based malware detection on top of allowlisting.
- Ensure your endpoint protection systems are armed with real-time threat intelligence gained from internal and external sources that cross organizational boundaries, geographies, and industries.

Restrict and manage external network access.

- Direct external remote desktop access should be disabled by default. If external access is necessary, ensure all administrative connections are conducted through an enterprise-grade, multifactor authentication VPN.
- Limit user privileges wherever possible, including users of bring-your-own-device (BYOD) initiatives.

Know your environment.

- Maintain an up-to-date inventory of all assets. Routinely validate the inventory and accounts associated with each device.
- Establish a network norm and set alerts for activity occurring outside of normal operations globally.
- Identify all traffic on the network and block all high-risk traffic.
- Review and inspect protections on all internet-exposed services.

How Cortex Helps Prevent, Detect, and Stop Ransomware Attacks

Cortex XDR® and Cortex XSIAM® deliver an integrated platform for cross-data prevention, detection, and response (figure 2). It lets your security team instantly contain network, endpoint, and cloud threats from one console. Analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists like bad domains through tight integration with enforcement points. Cortex XDR also allows you to:

- Use the Cortex XDR agent to block ransomware attacks at every step in the attack lifecycle, from the initial exploit to file analysis and behavioral protection.
- Find stealthy attacks with AI and cross-data analytics.
- Quickly investigate with root cause analysis.
- Contain any threat with a coordinated response.

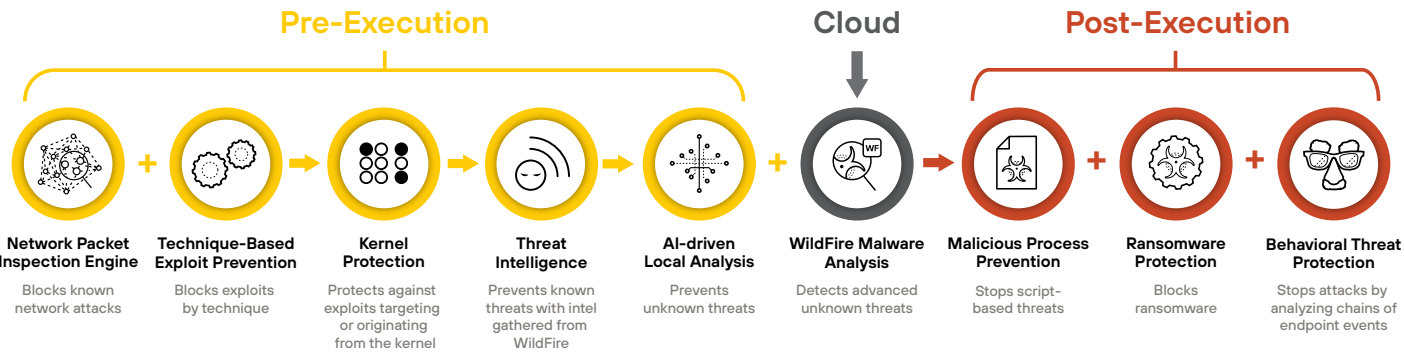

Figure 3: The XDR agent layers multiple methods of threat prevention for highly effective defense against ransomware

Response options in Cortex XDR and XSIAM include:

- **Live Terminal** for direct endpoint access includes a graphical task manager and file manager to view and terminate processes, delete files, download files, run commands, and much more.
- **Script Execution** from our management console to execute virtually any Python script on one endpoint, a group of endpoints, or all endpoints.
- **Search and Destroy** indexes all the files on your endpoints to find and delete malicious files anywhere in your organization in real time.
- **Remediate changes** to restore and revert changes made to your endpoints as a result of a malicious activity.

Why Traditional Endpoint Protection and Endpoint Detection and Response Aren't Enough

- Can't identify and block advanced endpoint attacks.
- Requires too many manual processes.
- Provides a limited, endpoint-only view into your environment.
- Depends on experienced analysts to manually investigate alerts.
- Weak at identifying new and advanced threats.

With our remediation suggestions, you can delete malware, restore files using Windows shadow copy, and remove registry key changes. These features are in addition to more traditional response options like quarantine, network isolation, blocking files, and integrating with Cortex XSOAR® for an automated response.

Five Musts If You've Been Attacked

1. **Network isolation**. Disable your virtual network interface card (NIC).
2. **Carefully consider the location of your attack info before rebooting**. Sometimes the encryption key and other attack info can be found in memory.
3. **Verify adequate data backups** and determine the overall risk to the organization if you don't pay the ransom.
4. **See if a decryption tool exists** using https://www.nomoreransom.org/.
5. **Execute an IR plan or call an IR team such as Palo Alto Networks Unit 42**. Unit 42 brings together an elite group of cyber researchers and incident responders with a deeply rooted reputation for delivering industry-leading threat intelligence. If you think you may have been breached or have an urgent matter, get in touch with the Unit 42 Incident Response team by emailing **unit42-investigations@paloaltonetworks.com** or calling:
   - **North America Toll-Free**: +1.866.486.4842 (+1.866.4.UNIT42)
   - **EMEA**: +31.20.299.3130
   - **APAC**: +65.6983.8730
   - **Japan**: +81.50.1790.0200

For more information on how Palo Alto Networks can help prevent ransomware attacks and/or minimize damage if a breach has occurred, view our on-demand webinar Best Practices for Stopping Ransomware and download our 2023 Unit 42 Ransomware and Extortion Report.

Defending against ransomware attacks starts with having a plan. Organizations can jump-start that process with our Ransomware Readiness Assessment.

Stay in the Know

As we've explored, preventing ransomware requires a multifaceted approach combining advanced technology, proactive strategies, and continuous vigilance.

For more information on Cortex XDR and Cortex XSIAM, please check out the following resources:

Cortex XDR

Visit our webpage.

Download our XDR For Dummies® guide.

Watch our video about How Cortex XDR works.

Cortex XSIAM

Visit our webpage.

Download our SOC transformation infographic.

Download our XSIAM solution brief.

Take the XSIAM product tour.

To learn more about the Cortex® portfolio of solutions, please visit our homepage.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_wp_surviving-ransomware_101624