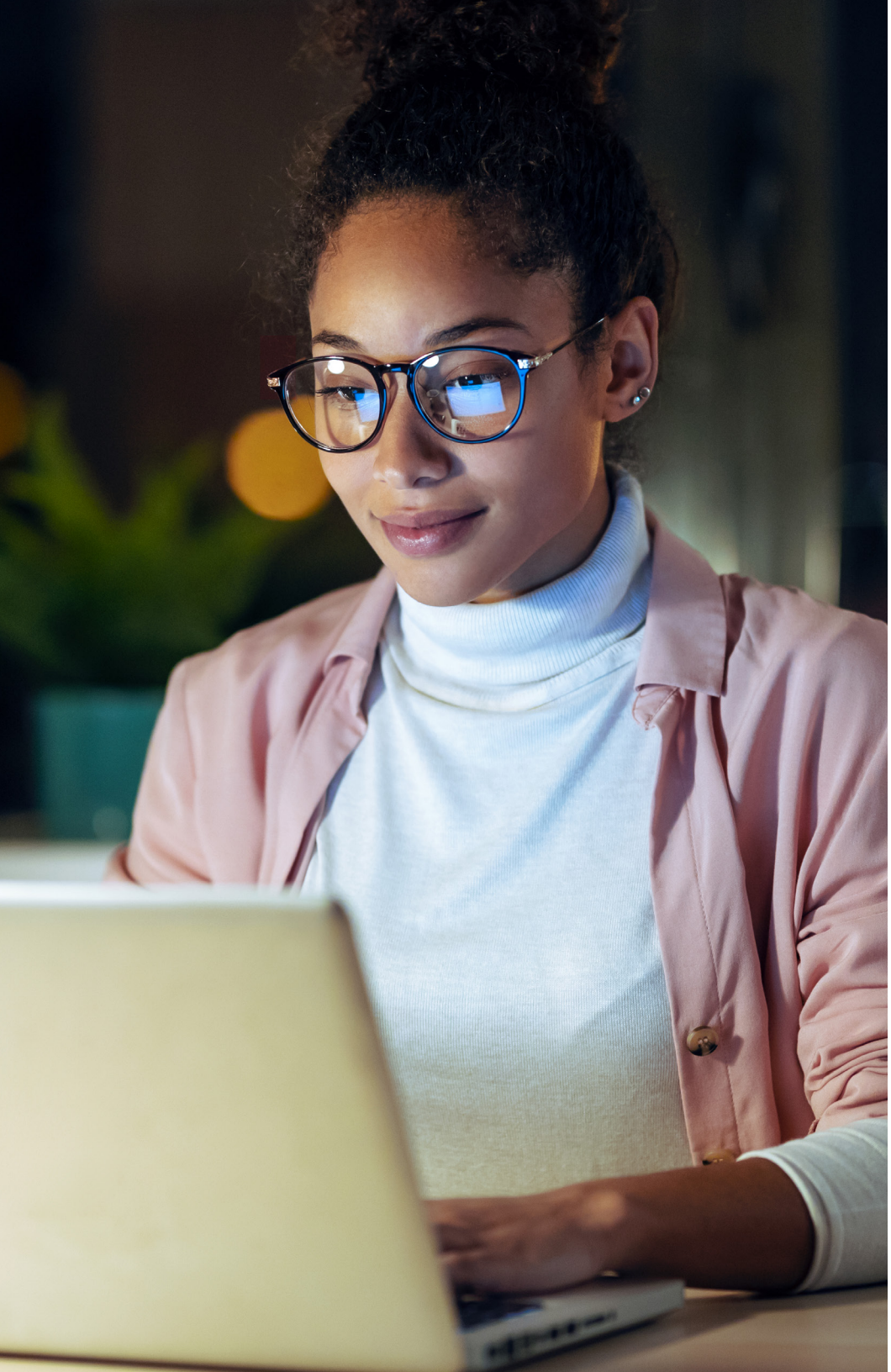
Healthcare Ransomware: What to Do Before, During and After an Attack

How to prevent system lockdowns, maintain patient care, and reduce the likelihood of a ransomware attack

By Marc Moring, Director of Strategic Accounts, Tanium

Table of Contents



Executive Summary: Take Action Before It's Too Late

Ransomware attacks are on the rise. In 2020, providers experienced more ransomware attacks; cybercriminals demanded larger ransoms; and a higher percentage of providers paid the ransoms. Worst of all, in 2020, the first patient died from a ransomware attack.

This surge won't subside. Yes, cybercriminals have increased their attacks against providers since COVID-19 struck. But they've targeted providers with escalating ransomware attacks for years. This trend won't stop when the pandemic stops.

Healthcare providers must fight back. Providers commonly develop ransomware defenses only after they've suffered a breach. This approach is too little too late. Providers must develop their ransomware defenses before they're targeted — and forced to pay.

This ebook will teach you how to do just that. It will dive deep into:

- The specific reasons why cybercriminals target healthcare providers with ransomware attacks, why current approaches to defending against ransomware don't work, and why healthcare providers must take a proactive approach to mature their ransomware defenses.
- The typical attack pattern you'll see if you suffer a ransomware campaign, the exact tactics you must deploy at every stage of that campaign, and the five steps you can take to develop an effective ransomware defense ASAP.
- The role that proper tooling plays in effective ransomware defense, why providers deploy legacy tools that can't defend them against ransomware, and how Tanium has delivered effective ransomware defense for providers.

Why Healthcare Organizations Must Defend Against Ransomware

The Surging Threat: Why Healthcare Must Address Ransomware

It's time to take ransomware seriously.

Daily attacks increased 50% year-over-year in Q3 2020.[1]

Ransoms are rising from $5,000 in 2018 to $200,000 in 2020.[2]

Patient care is being disrupted, with potentially fatal consequences.

In 2020, the first patient died due to a ransomware attack.[3] The patient was in urgent care, and a ransomware attack shut down the healthcare provider. The provider transferred the patient, but the closest hospital was 20 miles away. The patient died in transit.

Ransomware is a real threat to providers, patients, and society, and it's growing more severe. Here's why.

Easy Money: Why Criminals Target Healthcare Providers

It's tempting to blame the rise of healthcare ransomware attacks on COVID-19 and believe this threat will subside when the pandemic eventually fades away. There's some truth to this.

Criminals did increase their ransomware attacks against healthcare providers when the pandemic struck and overwhelmed the medical system. And these attacks may die down a bit when the pandemic subsides and providers are less overwhelmed.

But the ransomware threat didn't begin with COVID-19 — and it won't go away.

Hospitals were already a primary and growing target for ransomware attacks before the pandemic. Attacks against providers rose 350% in Q4 2019 alone.

Ultimately, criminals target healthcare providers for deeper reasons than the pandemic.

Providers have fundamental vulnerabilities that make them easy targets for ransomware attacks, and the pandemic only made these vulnerabilities worse.

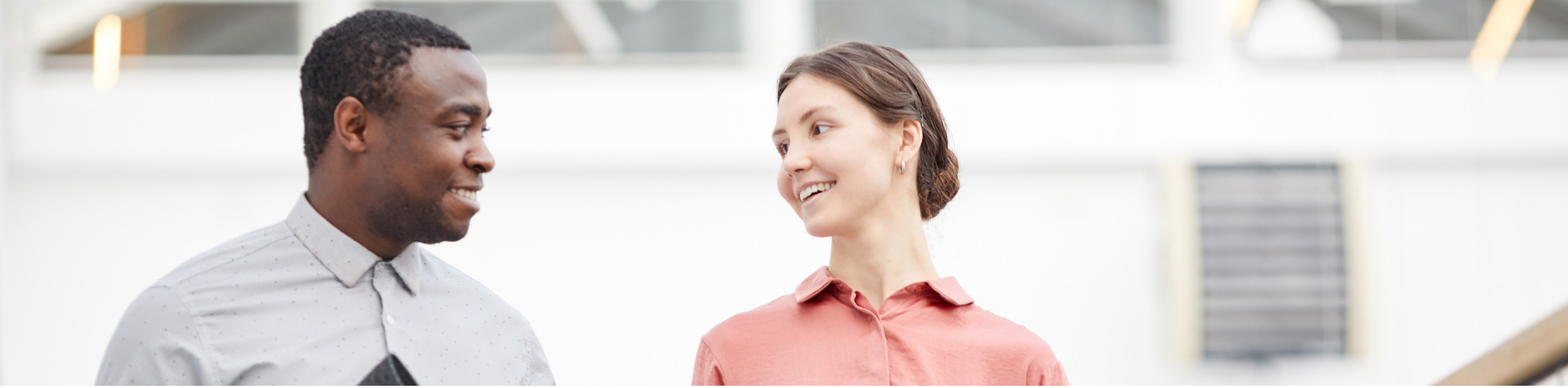
Attacks against providers rose 350% in Q4 2019 alone.

Most healthcare providers are vulnerable to ransomware because they:

- **Focus on patient care, not cybersecurity.** Most healthcare leaders are former clinicians and don't make cybersecurity a top priority.
- **Use outdated, compliance-driven security.** Providers build security to meet the bare minimum requirements, which haven't evolved to address ransomware.
- **Have poor visibility and IT hygiene.** Providers don't know what assets are in their environment and leave many of those assets with open exploits.
- **Are willing to pay.** Because providers can't compromise patient care or evict attackers, they commonly pay ransoms quickly to restore their operations.

These vulnerabilities existed before COVID and will remain after COVID. Healthcare providers can't wait out the pandemic and hope the current wave of ransomware attacks will eventually end. They must take a proactive approach to ransomware and develop defenses before they become victims.

Unfortunately, very few healthcare providers take this approach.



Too Little, Too Late: Why Current Responses to Ransomware Fail

To date, many healthcare providers have taken a reactive approach to ransomware. They've attempted to upgrade their defenses in only one of two scenarios:

- **They heard a wave of ransomware attacks were imminent.** They received a warning from researchers that attacks were coming and scrambled to respond.

OR

- **They already suffered a ransomware attack.** They were forced to pay and then decided to build their defenses after the incident.

In each scenario, a reactive response is the wrong approach.

Ransomware moves fast, and it's impossible to build defenses reactively. Ransomware has been able to compromise a provider in less than one hour.

In one instance, a criminal exploited a single unmanaged piece of biomedical equipment. The criminal then moved laterally and infected more than 8,000 other endpoints with ransomware — all in approximately 45 minutes.

This is a typical ransomware attack. This is what you must build defenses against. And this is why you must already have those defenses in place before criminals strike. Here's how you can begin to do that.

First Steps: Begin to Build Your Defenses Against Ransomware

To defend against ransomware before an attack strikes, you must consider these essential steps:

1. Make ransomware a priority. Ransomware has become a critical factor in patient care. You must address it to maintain core operations.
2. Extend security beyond compliance. Criminals evolve faster than regulations. You must not rely on regulations to protect you.
3. Establish complete visibility and IT hygiene. Doing so reduces the chance of a breach and makes it possible to detect attacks and remediate them.
4. Develop a strong negotiating position. You must feel confident that you can evict criminals and resolve attacks quickly — without having to pay.

How Healthcare Providers Can Defend Against Ransomware

To bring these steps to life, you'll need to develop a suite of security capabilities. This section outlines what those capabilities are and how to build them.

It will explore:

- What a typical ransomware attack looks like and how it progresses.
- What tactics you must employ to resolve ransomware without paying.
- How you can build an effective defense against ransomware in five steps.

Understanding Ransomware: Looking Beyond the Ransom Note

On the surface, a typical ransomware attack looks simple. A healthcare provider tries to log into a workstation. The systems are locked up. The provider can't log in and, instead, sees a message.

The message is from an attacker and tells the provider to pay a ransom to restore systems and save data. The provider pays the ransom or evicts the attacker, and the attack is over.

This description is mostly accurate, but it's incomplete. The attacker had to perform a significant number of steps before the attack. The attacker might also extend the attack campaign even after getting paid or evicted. A more comprehensive picture of a ransomware attack is outlined to the right.

Profile of a Ransomware Attack

Before the Attack

The attacker develops the necessary intelligence, control and leverage to put the provider in a challenging position.

The attacker follows these steps:

- Scan the provider's network for vulnerabilities.
- Launch standard attacks — like phishing — or exploit known vulnerabilities — like unpatched assets.
- Move laterally through vulnerable systems.
- Develop a foothold in the environment.
- Gather intelligence on critical systems.
- Exfiltrate as much sensitive data as possible.
- Develop the ability to take control of provider systems.

During the Attack

The attacker creates as many problems for the provider as possible and sends the provider the ransom note.

The attacker follows these steps:

- Lock every critical system under the attacker's control.
- Threaten to dump sensitive data the attacker stole.

After the Attack

The attacker may launch additional attacks. In many cases, paying a ransom makes an attacker more likely to strike again.

The attacker follows these steps:

- Maintain a hidden foothold in the environment.
- Exploit other network vulnerabilities discovered in the previous attack.
- Exfiltrate more data.
- Eventually lock systems, threaten to dump data again, and demand another ransom.

In short, by the time an attacker demands a ransom, it's commonly too late. The attacker has already spent days, weeks, or even months preparing for the attack.

By the time an attacker demands a ransom, it's commonly too late. The attacker has already spent days, weeks, or even months preparing for that moment.

And at that point, the healthcare provider must face some harsh truths. The provider:

- Lacked the capabilities to defend against the attack's progression
- Most likely doesn't have the capabilities to confidently evict the attacker
- Will have to pay up and hope the attacker doesn't strike again

Here's how you can prevent this scenario from happening.

Defending Against Ransomware: There's No Silver Bullet

No single tactic can defend against ransomware. Any effective defense must be as complex and multifaceted as the attack. Healthcare providers must use a wide range of defensive capabilities at every step of the attacker's campaign.

An effective anti-ransomware security posture must include the steps outlined to the right.

In short, there's a lot of work to do to defend against ransomware. Many healthcare providers can't perform at least a few of these tactics. Some can't perform any of them.

But all healthcare providers must — at the very least —start that process.

An Effective Anti-Ransomware Security Posture

Before the Attack

The provider must raise the barrier to entry to its network and reduce the chance of suffering an opportunistic attack.

The provider should:

- Establish continuous visibility into endpoints — including applications and the activity on them.
- Remove known vulnerabilities on assets by constantly patching, updating, and configuring them.
- Proactively hunt for indicators of compromise as evidence of in-progress attacks before they develop further.

During the Attack

The provider must remediate the attack and evict the attacker quickly.

The provider must:

- Investigate the attack to identify its root cause, its lateral spread, and everything the attacker touched.
- Close remaining vulnerabilities in the environment to contain the attack's further spread.
- Remediate the attack, evict the attacker, and regain control of its systems without significant data loss.

After the Attack

The provider must harden the environment and help ensure the attacker is truly gone and can't compromise the network again.

The provider must:

- Find instances of each vulnerability the attacker exploited and close them on assets.
- Find any remaining foothold the attacker might still have and evict them.
- Continuously improve the overall health and security of the endpoint environment to prevent new attacks.

What to Do: Five Steps to Building an Effective Ransomware Defense

If you follow these steps, you'll:

- Identify the gaps in your current ransomware defense capabilities.
- Fill in the most critical gaps that you might uncover.
- Develop a strong ransomware defense, even if you start from nothing.

Step One: Assess Your Current Ransomware Defenses

First, ask yourself a few questions to determine your current ability to defend against ransomware threats at every stage of an attack.

Ask yourself:

- Do we have an accurate catalog of every asset in our environment?
- Can we monitor those assets and search for specific indicators of compromise (IoCs) on them?
- Are these assets patched, updated, and configured at all times?
- How quickly can we detect a compromised asset or other threat?
- Can we determine every asset and piece of data an attacker touched?
- How quickly could we contain and remediate an incident?
- Can we evict an attacker with % confidence that they're gone?
- How fast could we harden our environment against similar attacks?

Finally, ask yourself:

- Could we detect and remediate a ransomware attack before it compromised our ability to provide patient care — or would we have to pay the ransom?

Step Two: Develop Comprehensive Visibility Into Your Assets

First, in terms of priority, you must fill any visibility gaps you identify. Visibility provides a foundation and force multiplier for all other activities.

You must develop the visibility to:

- Identify the endpoints in your environment and the software on them.
- Identify the current status of patches, software versions, configuration settings, administrative rights, and known vulnerabilities on each of those assets.
- Continuously monitor the behavior of those assets and their users.
- Define each asset's measurable risk and map the potential trajectory and impact if a successful ransomware attack were to occur.

Visibility provides a foundation and force multiplier for all other activities.

You must develop the ability to do so for managed and unmanaged assets, regardless of whether they live on-premises or off.

Step Three: Button Up Your Approach to IT Hygiene

Next, you have to focus on improving your IT hygiene. Most ransomware attacks exploit known vulnerabilities in the environment.

You must maintain good IT hygiene and a high barrier to entry. To maintain good IT hygiene, you should be able to:

- Maintain high patch compliance and rapidly apply new patches to all assets.
- Keep all software and operating systems up to date with the latest versions.
- Enforce policy, access rights, and configurations on all assets.
- Maintain compliance with all your regulatory requirements.

You must perform these actions remotely, at scale, and within a closed-loop verification system that ensures correct application of your controls.

Step Four: Establish Your Incident Response Capabilities

Next, ensure your visibility and control mechanisms extend beyond prevention. You should be able to employ them to rapidly stop attacks and evict attackers.

To respond to a ransomware incident, you must be able to:

- Detect attacks before they strike — including unknown, unpredictable attacks.

- Combine real-time and long-term data to define attack chains.
- Remediate incidents before the attacker locks systems and exfiltrates data.
- Learn from incidents and proactively raise defenses against similar patterns.

You should be able to perform each of these actions in near real-time to respond effectively to the rapid spread of most modern ransomware attacks.

Step Five: Reevaluate Your Tooling

Finally, take a hard look at your endpoint tools. Your tools are the basis for every capability in this ebook.

If you have a gap in any of them, you most likely:

- Haven't deployed a tool to deliver that capability.

OR

- Have deployed the wrong tool for your modern environment.

Look at the tools you deploy to deliver visibility, IT hygiene, and incident response. Make a list of any that don't deliver value during your day-to-day work.

Then, for each tool, ask yourself one final question:

If these tools can't deliver value under normal circumstances, will they deliver the value I need in the middle of a ransomware incident?

Any tool that receives a "no" is ripe for replacement.

How Healthcare Organizations Can Deploy the Right Tools to Stop Ransomware

The final section of this ebook will discuss tools in depth. It will show you how to select security tools that can defend against ransomware.

It will explore:

- Why healthcare providers cannot defend themselves with legacy tools
- How Tanium corrects the fundamental problems with legacy tools
- How multiple healthcare providers have used Tanium to improve their security

New Problem, Old Solution: Why Legacy Tools Fail Against Ransomware

Ransomware moves fast. If you suffer an attack, you won't have time to spin up new security tools. You'll have to defend against the attack with the tools you have in place.

If you have the right tools, you'll be able to stop the attack and evict the attacker. If you have the wrong tools, you'll be forced to deal with the fallout of the attack.

Unfortunately, the legacy security systems that most healthcare providers use are commonly the wrong tools to defend against ransomware.

The problem is simple. Legacy tools were designed to secure legacy healthcare environments. Those legacy environments were:

- **Small.** Healthcare providers deployed a relatively low volume of assets. They still did most work manually and didn't use too many devices or applications.
- **Simple.** Assets were provisioned by IT and lived on-premises. IT knew what assets were in the environment at all times and what they were doing.
- **Static.** Healthcare asset environments didn't change too often. Any new device, application, or update was provisioned slowly and with oversight.

At the same time, legacy healthcare environments faced relatively predictable, unsophisticated threats and required fewer capabilities to defend against them.

But times have changed. Healthcare providers now operate in modern IT environments. These digital infrastructures are:

- **Large.** Healthcare providers now deploy a large volume of assets. Frontline workers perform most of their work on devices and applications.
- **Complex.** These assets are commonly provisioned by users and live off-network. IT doesn't know what assets are in their environment or what they're doing.
- **Chaotic.** Healthcare asset environments change rapidly. New devices, applications, and updates are deployed quickly and without IT's knowledge.

Modern healthcare environments face threats like ransomware that are unpredictable, sophisticated, and require many capabilities to remediate.

And when healthcare providers attempt to use legacy tools to defend their modern environments against threats like ransomware, those tools typically fail. They deliver stale data that leaves blind spots for attackers to hide in. They can't perform simple actions like patches and updates to their assets.

And they force healthcare providers to deploy a large number of isolated point solutions that are expensive and complex to stand up and don't work well together.

Very simply, legacy tools fail because they were designed for legacy environments. To defend their modern asset environments, providers must deploy modern tools. Tools like Tanium.

Meet Tanium: A Modern Security Solution for Ransomware

Tanium was designed to help secure modern asset environments.

Legacy tools fail because they were designed for legacy environments. To defend their modern asset environments, providers must deploy modern tools.

Tanium takes a different approach when compared with most healthcare organizations' current strategies. The Tanium platform addresses the challenges healthcare providers face when leveraging legacy tools to secure and manage their modern asset environments against ransomware.

By using Tanium against ransomware, healthcare providers can:

Develop comprehensive visibility into their assets. Tanium uses unique methods to find "hidden" assets that legacy tools miss. Providers typically discover 10%–20% more assets than they knew they had. Tanium performs continuous scanning of the asset environment to establish and maintain real-time visibility into devices, applications, and users.

Tanium uses unique methods to find "hidden" assets that legacy tools miss. Providers typically discover 10%–20% more assets than they knew they had.

Establish and maintain near-perfect IT hygiene. Tanium employs distributed edge computing to apply and validate large-scale patches, updates, configurations, and other fundamental controls. For example, Tanium can produce 99% patch visibility within 24 hours of installation.

Perform incident response with a single, unified platform. Tanium provides a unified platform that offers most of the core capabilities required to detect, investigate, and remediate ransomware threats in one tool. These capabilities work well together, operate from the same data, and drive a collaborative response.

In short, Tanium provides a holistic defense against ransomware attacks.

And this solution isn't theoretical. Many healthcare providers already deploy Tanium to help secure their asset environments.

Here are a few examples:

One provider needed to quickly and easily discover and report on medical devices in the environment, while also increasing patch compliance past 70%. The provider used Tanium to augment Microsoft System Center Configuration Manager (SCCM) deployment and discover the medical devices in its environment and rapidly patch those systems.

One provider knew there were 20,000+ assets in the environment and approximately 25% of them were unmanaged. The provider used Tanium to bring these unmanaged assets under control. The provider also found many unknown assets in the environment and learned 75% of the assets had open vulnerabilities.

Tanium provides a unified platform that offers most of the core capabilities required to detect, investigate and remediate ransomware threats in one tool.

One provider couldn't perform effective crisis management due to a lack of comprehensive visibility into assets. The provider used Tanium to account for the endpoints, proactively hunt for malware, and deliver real-time forensic data to an SIEM tool for incident analysis.

Security leaders at these healthcare providers applied a wide range of Tanium's capabilities to raise their defenses against ransomware. They found the solution outlined in the table below to be the most effective.

Asset Discovery and Inventory
Know what endpoints and applications are in the environment, even as the environment rapidly changes.

Patch and Software Management
Apply large-scale patches and software installations and updates to distributed endpoints in minutes or hours.

Vulnerability and Configuration Management
Find open vulnerabilities, breaks in compliance, and policy misconfigurations and remediate issues.

Incident Response
Leverage a comprehensive suite of unified capabilities to rapidly detect, investigate, and remediate incidents.

Healthcare providers could spin up these solutions rapidly by leveraging Tanium's single-agent, lightweight architecture, and cloud-based offering.

Through Tanium, they gained a unified platform that contained the core security capabilities. They used Tanium to fill the gaps in their existing security posture or spin up a new, end-to-end ransomware defense from a single solution.

Build your defense against ransomware starting today.

So far, we've outlined a comprehensive strategy to combat ransomware:

- **First, take a proactive approach.** Ransomware is growing in frequency and impact. Ransomware attacks are crippling major organizations in every industry. You must build defenses before you're targeted.
- **Second, develop the right capabilities.** Ransomware is a complex, multistage attack. There's no one silver bullet. To combat it, you must develop real-time visibility, pristine IT hygiene, and incident response capabilities.
- **Finally, deploy modern security tools.** Legacy tools can't secure modern environments against fast, complex threats like ransomware. You must deploy tools built to match the speed and scale of your modern asset environment.

Now, it's time to act.

Review your ability to defend against ransomware. Kick-start your plans to develop the capabilities to combat this threat. And reach out to see if Tanium is the right platform to help you secure your network and endpoints against ransomware attacks.

---

[1] Davis, J. (2020). "US ransomware attacks doubled in Q3: Healthcare sector most targeted" [Online]. Accessed on the Web at https://healthitsecurity.com/news/us-ransomware-attacks-doubled-in-q3-healthcare-sector-most-targeted

[2] Newman, L. H. (2020). "Ransomware is headed down a dire path" [Online]. Access on the Web at https://www.wired.com/story/ransomware-2020-headed-down-dire-path/

[3] Cimpanu, C. (2020). "First death reported following a ransomware attack on a German hospital" [Online]. Accessed on the Web at https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/