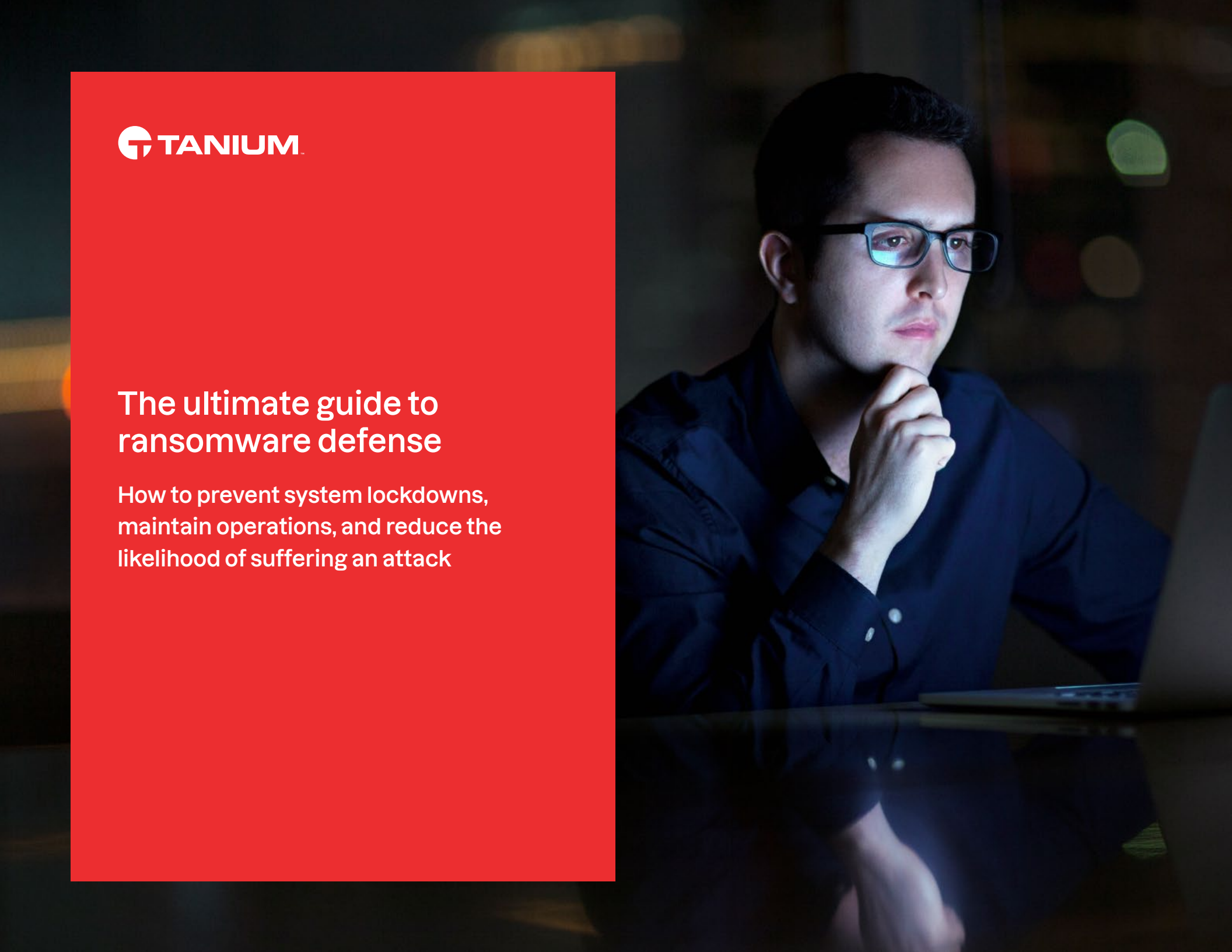

TANIUM

The ultimate guide to ransomware defense

How to prevent system lockdowns, maintain operations, and reduce the likelihood of suffering an attack

TANIUM

The ultimate guide to ransomware defense

How to prevent system lockdowns, maintain operations, and reduce the likelihood of suffering an attack

Contents

EXECUTIVE SUMMARY

Act before it's too late

Ransomware has become one of the most common, high-impact threats in the cybersecurity landscape. Ransomware attacks are more expensive than other types of breaches; the cost and frequency of these attacks are increasing; and every industry has suffered high-profile incidents.

All organizations must now consider themselves a potential target for this threat and build an effective defense against it before they suffer an incident.

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

- The typical attack you'll see if you suffer a ransomware campaign
- The exact tactics you must deploy to defend your organization at every stage of a ransomware campaign — before, during, and after the attack
- The five steps you can take to develop an effective ransomware defense ASAP
- The role that proper tooling plays in building an effective ransomware defense
- Why legacy security tools typically fail to defend modern environments against ransomware
- How Tanium corrects the failings of legacy tools and the role this solution can play in building an effective and efficient defense against ransomware — fast
- How Tanium has delivered effective security for many organizations
- How to leverage Tanium to augment or develop your ransomware defense

Why now is the time to take ransomware seriously

Ransomware is more expensive than other cybersecurity threats.

The Ponemon Institute's most recent Cost of a Data Breach Report found that the average overall cost of a ransomware breach was $250,000 more than the average overall cost of a standard malicious breach.[1]

$4.27 million

Overall average cost of a malicious breach.

$4.52 million

Overall average cost of a ransomware breach.

Ransomware is growing even more expensive and more frequent.

The FBI's most recent Internet Crime Report found that from 2018 to 2019 ransomware attacks became more common and generated greater losses.[2]

37%

annual increase in reported ransomware cases

147%

annual increase in associated losses from ransomware attacks

Further, Cybersecurity Magazine projects the rate of ransomware attacks has more than tripled in the past five years, and the global estimated damages have more than doubled.[3]

Ransomware attack rate

40 seconds

Attack rate in 2016

14 seconds

Attack rate in 2019

11 seconds

Attack rate in 2021 (projected)

Global estimated damages from ransomware attacks

$8 billion

In 2018

$11.5 billion

In 2019

$20 billion

In 2021 (projected)

Ransomware is becoming a problem for every industry.

In recent years, every industry has experienced high-profile ransomware breaches.

A few examples:

- **Healthcare:** In September 2020, a hospital chain with 400 locations appeared to be hit in the largest healthcare ransomware attack in U.S. history.[4]
- **Government:** In 2019, the City of Baltimore suffered a ransomware attack that cost it more than $18 million and suspended municipal services.[5]
- **Education:** Ransomware attacks impacted more than 85 higher education institutions and disrupted operations for more than 1,200 schools in 2020.[6]
- **Technology:** An IT services company was hit with a Maze ransomware attack in 2020 that was projected to cost it $50 to $70 million in overall impact.[7]
- **Retail:** In December 2020, Kmart experienced a ransomware attack that disrupted services in the middle of the holiday shopping season.[8]

No one is safe from ransomware. Every organization must see itself as a potential target and build effective defenses against this attack pattern before it becomes the next major victim. This eBook outlines a clear, practical path toward building those defenses.

How organizations can defend themselves against ransomware

This section details an effective security strategy to combat ransomware and how to bring this strategy to life.

It will explore:

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

Understanding ransomware: Looking beyond the ransom note

On the surface, a ransomware attack looks simple. An organization's employees try to log into their workstations. Their systems are locked up. They can't log in. Instead, they see a message.

The message is from an attacker and tells the organization to pay a ransom to restore systems and save data. The organization either pays the ransom or evicts the attacker, and the attack is over. This description is mostly accurate, but it's incomplete.

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.

The attacker had to perform a significant number of steps before the attack. The attacker might also extend the attack even after they're paid or evicted. A more comprehensive picture of a ransomware attack emerges as outlined to the right.

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 organization faces some harsh truths. The organization:

- 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. Organizations must use a wide range of defensive capabilities at every step of the attacker's campaign.

In short, there's a lot of work to do to defend against ransomware. Many organizations are unable to perform at least a few of these tactics. Some are unable to perform any of them.

But all organizations must start the process.

Profile of a ransomware attack

Before the attack

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

The attacker follows these steps:

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

During the attack

The attacker creates as many problems for the organization as possible and sends the organization a 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.

An effective anti-ransomware security posture

Before the attack

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

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

The organization must:

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

After the attack

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

The organization must:

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

What to do: Five steps to building an effective ransomware defense

If you follow these steps, you can:

- Identify the gaps in your current ransomware defense capabilities.
- Fill in the most critical gaps 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:

- 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 most critical operations — or would we have to pay the ransom?

Step two: Develop comprehensive visibility into your assets.

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

You must develop visibility over the assets in your environment — whether they're managed or unmanaged, and whether they live on-premises, on remote networks, or move on and off network.

For each of these assets, you must develop the visibility to:

- Identify their hardware as well as the software on them.
- Review the current status of their patches, software versions, configuration settings, administrative rights, and known vulnerabilities.
- Establish a baseline for normal behavior of those assets and their users, continuously monitor current behavior against that baseline, and trigger alerts when abnormal behavior occurs.
- Define each asset's measurable risk and map the potential trajectory and impact if a successful ransomware attack were to occur.

You must develop a comprehensive, accurate, up-to-date asset inventory. Your inventory should be resilient to changes in your environment. And you must be able to rapidly query any asset — or group of assets — within your inventory for specific vulnerabilities or indicators of compromise (IoCs).

Step three: Button up your approach to cyber hygiene.

Next, you must focus on improving your cyber hygiene. Most ransomware attacks exploit known vulnerabilities in the environment.

You need to maintain good cyber hygiene and a high barrier to entry at all times. So, you must be able to close known vulnerabilities on your assets remotely, at scale, and within a closed-looped system that ensures correct application of controls.

To maintain good cyber hygiene on your assets, you should be able to:

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

You must achieve near-perfect compliance with each of these controls. An attacker needs to find and exploit only one vulnerability on one asset to breach your network and initiate a ransomware campaign. You can no longer accept compliance rates of 70%, 80%, or even 90% as "good enough."

Step four: Establish your incident response capabilities.

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

To respond effectively to the rapid spread of most ransomware attacks, you should be able to perform a wide range of visibility and control capabilities in near real-time across your entire environment.

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

- Test your response plans to know how you'll react during an incident.
- Detect attacks before they strike, including unknown, unpredictable attacks.
- Combine real-time and long-term data to define attack chains.
- Know precisely what the attacker touched, accessed, and compromised.
- Remediate incidents before the attacker locks systems and exfiltrates data.
- Determine if the attacker still has a foothold in your asset environment.
- Learn from incidents and proactively raise defenses against similar patterns.

You can perform the above actions at speed and scale only if they're consolidated within a single platform. During an incident, you won't have time to juggle multiple tools, teams, and data sets. You'll need streamlined, collaborative processes that operate from a single source of truth and a shared toolset.

Step five: Re-evaluate your tooling.

Finally, take a hard look at your endpoint tools. They're the basis for every capability in this eBook. If you have a gap in any of these capabilities, you most likely:

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

OR

- Have deployed the wrong tool for your environment.

Look at the tools you deploy to deliver visibility, cyber 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 cannot 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 organizations can deploy the right tools to stop ransomware

This section will discuss tools in depth. It will show you how to select security tools that can defend against ransomware.

It will explore:

- Why organizations cannot defend themselves with legacy tools.
- How Tanium corrects the fundamental problems with legacy tools.
- How multiple organizations 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 organizations use are commonly the wrong tools to defend against ransomware.

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

- **Small.** Organizations 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.** Organizational asset environments didn't change too often. Any new device, application, or update was provisioned slowly and with oversight.

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

But times have changed. Organizations now operate modern IT environments.

These digital infrastructures are:

- **Large.** Organizations now deploy a large volume of assets. Employees now perform most of their work on devices and applications.
- **Complex.** 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.** Asset environments change rapidly. New devices, applications, and updates are deployed quickly and without IT's knowledge.

Moreover, modern organizations face threats like ransomware, which are unpredictable, sophisticated, and require many capabilities to remediate. When organizations 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.

They can't quickly, efficiently, or confidently evict attackers when incidents do occur. And they force organizations 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're designed for legacy environments. To defend modern environments, organizations must deploy modern tools. Tools like Tanium.

A modern security solution for ransomware

Tanium was designed to help secure modern environments.

Tanium takes a different approach when compared with the current strategies of most organizations. The Tanium platform addresses the challenges organizations face when using legacy tools to secure and manage their environments.

Tanium employs a lightweight, distributed architecture. This architecture means that Tanium can perform the core activities of ransomware defense on centralized and remote environments — no matter how many assets they contain — without creating meaningful network strain.

By using this modern architecture, Tanium can effectively secure large, complex, chaotic asset environments against threats like ransomware.

By using Tanium against ransomware, organizations can:

Develop comprehensive visibility into their assets.

Tanium uses unique methods to find "hidden" assets that legacy tools miss. When organizations first launch Tanium, they typically find 10% to 20% more assets than they knew they had. Tanium creates visibility into the applications, users, access rights, configurations, and known vulnerabilities on each of those assets as well as the measurable risk that each asset generates.

Then Tanium maintains this visibility. Tanium can perform continuous, real-time scanning of the asset environment and tell organizations everything that's occurring on their endpoints at any given moment.

Establish and maintain near-perfect cyber hygiene.

Tanium employs distributed edge computing to apply large-scale patches, updates, configurations, and other fundamental controls in minutes, hours, or days — instead of weeks or months. Tanium validates the application of these controls and can double back to correct any misapplications.

Tanium can produce 99% patch visibility within 24 hours of installation. From there, Tanium can rapidly apply new controls to assets, maintaining near-perfect hygiene.

Perform incident response within 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 to threats — while eliminating the cost and complexity of deploying multiple point tools.

Organizations can combine multiple Tanium capabilities to

detect and investigate complex attack chains, remediate incidents in near real-time, and confidently evict attackers and harden their defenses against similar attacks.

How Tanium addresses ransomware at every stage of the attack

As shown in the right column, Tanium provides a complex, multistage defense against ransomware, with a wide range of defensive capabilities to counter every stage of the attacker's campaign from a single, unified platform.

Tanium can combat ransomware at every stage of the attack, which means organizations can use Tanium for ransomware in one of two ways:

- They can use Tanium as their central hub to defend against ransomware.

OR

- They can use Tanium to fill the gaps in their current security system.

Tanium is a flexible, extensible platform with open API integrations. It works out-of-the-box with many other security vendors and orchestration platforms. Organizations can use Tanium's data to aggregate, centralize, and analyze endpoint metrics as part of a broader security strategy and larger ecosystem of anti-ransomware tools.

How Tanium protects your organization against ransomware

Before the attack

Tanium creates near-perfect cyber hygiene in the most dynamic, diverse, and distributed asset environments.

Organizations can use Tanium to:

- Create a comprehensive, real-time inventory of endpoints including their software, users, and vulnerabilities.
- Patch, update, configure, or otherwise apply controls to hundreds of thousands of endpoints in hours or days.
- Perform continuous scans or real-time spot searches for specific indicators of compromise (IOCs) across endpoints.

During the attack

Tanium can investigate attacks in near real-time and rapidly apply controls to evict the attacker.

Organizations can use Tanium to:

- Define the source of the attack, map the entire attack chain, and identify assets the attack compromised.
- Identify what other assets the attack could spread to and harden them in real time against the pattern.
- Enter negotiations with the knowledge that they can evict the attacker before operations are compromised.

After the attack

Tanium can learn from the attack and harden the environment against a second strike or similar attack patterns.

Organizations can use Tanium to:

- Perform a spot search to find and close remaining instances of the vulnerabilities exploited in the attack.
- Scan the environment for remaining traces of the attackers and evict them with confidence.
- Continue to perform fundamental cyber hygiene at a high level to reduce the chance of suffering another breach.

Real clients, real results: How organizations have deployed Tanium

This solution isn't theoretical. Many organizations already deploy Tanium to secure their asset environments against a variety of cyberthreats, including ransomware. Here are a few examples.

Global law firm

"Our ability to respond to incidents was slower than we needed it to be. Tanium has made the team much faster."

CHALLENGE:

Meeting its heavily regulated client's security requirements for incident response, patching, and the like.

BEFORE TANIUM:

Incident response teams had to connect directly to compromised endpoints, requiring travel or shipment of the endpoint, and hours or days to complete the task.

AFTER TANIUM:

Endpoint visibility accelerated from weeks to minutes, and endpoint triaging and remediation activities now occur remotely, accelerating incident response.

Global retail group

"We can rely on Tanium to become our single point of visibility and control, to manage and secure our enterprise, and to bring new levels of investment efficiencies."

CHALLENGE:

Lack of visibility and manual incident remediation across a distributed global organization of 25,000 employees.

BEFORE TANIUM:

Inefficient endpoint protection that required up to a week to resolve critical issues, and left compromised machines exposed for days.

AFTER TANIUM:

Endpoint protection activities that required nearly one week to complete are now done in less than one day —in some cases in less than four hours.

Leading technology firm

"We can now automate what we know, to spend more time looking for what we don't know, and ultimately automate that."

CHALLENGE:

Teams were adept at identifying threats, but lacked comprehensive visibility into their environment, and faced challenges thoroughly investigating the threats they found.

BEFORE TANIUM:

Incident response teams used iterative threat hunting and investigation tools that took too long to scope threats, further delaying their response.

AFTER TANIUM:

Teams now investigate and respond to threats remotely in real time, dramatically reducing their mean-time-to-recover and accelerating their ability to close vulnerabilities.

Ransomware defense with Tanium: Essential solutions

While the security leaders at these organizations applied a wide range of Tanium's capabilities to raise their defenses against ransomware and other modern threats, they found the solutions outlined 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.

Risk and Compliance Management

Assess the risk and impact of exploits, including lateral movement, in real time.

Threat Hunting

Confidently answer the "Are we good?" question, knowing you can report back on any endpoint, anywhere — to fix incidents and prevent them from happening again in seconds.

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

With Tanium Cloud, organizations can launch new security capabilities in hours or days — not weeks or months — to rapidly fill the gaps in their existing security posture or to 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 silver bullet. To combat it, you must develop real-time visibility, pristine cyber 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.

Schedule a free consultation and demo of Tanium.

Schedule now →

Let Tanium perform a thorough cyber hygiene assessment of your current environment.

Get cyber hygiene assessment →

Launch Tanium with our cloud-based offering, Tanium Cloud.

Try now →

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at **www.tanium.com** and follow us on **LinkedIn** and **Twitter**.

TANIUM

References

1. Zorabedian, J. (2020). "What's new in the 2020 cost of a data breach report" [Online]. Accessed on the Web at https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
2. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) (2020). "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" [Online]. Accessed on the Web at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
3. Morgan, S. (2019). "Global ransomware damage costs predicted to reach $20 billion (USD) by 2021" [Online]. Accessed on the Web at https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
4. Collier, K. (2020). "Major hospital system hit with cyberattack, potentially largest in U.S. history" [Online]. Accessed on the Web at https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254
5. Torbet, G. (2019). "Baltimore ransomware attack will cost the city over $18 million" [Online]. Accessed on the Web at https://www.engadget.com/2019-06-06-baltimore-ransomware-18-million-damages.html
6. Srinivas, R. (2020). "Ransomware attacks in 2020! These are four most affected sectors" [Online]. Accessed on the Web at https://cisomag.eccouncil.org/ransomware-attacks-in-2020-these-are-4-most-affected-sectors/
7. Cimpanu, C. (2020). "Cognizant expects to lose between $50m and $70m following ransomware attack" [Online]. https://www.zdnet.com/article/cognizant-expects-to-lose-between-50m-and-70m-following-ransomware-attack/
8. Ballard, B. (2020). "Kmart is latest retailer to suffer major ransomware attack" [Online]. Accessed on the Web at https://www.techradar.com/news/kmart-is-the-latest-retailer-to-suffer-a-ransomware-attack