TANIUM

Stopping Today's Three Biggest Cyber Threats

How Security Leaders Are Defending Their Organizations Against the New Wave of Attacks

Table of Contents

The Mandate: Defend Against the New Wave of Attacks

The year 2020 opened massive opportunities for cybercriminals.

"What you have to understand about something as big as COVID-19 is that criminals aren't looking at it the way the rest of us are," says Jenny Radcliffe, Founder and Director at Human Factor Security. "We worry 'Will everyone be ok?'. But criminals are opportunists."

> *"Criminals aren't looking at COVID the way the rest of us are. Criminals are opportunists."*
>
> Jenny Radcliffe, Founder and Director, Human Factor Security

Cybercriminals took advantage of the chaos and confusion to launch more attacks, generate more breaches, compromise more organizations and make more money.

"I do a lot of incident response and forensics and the number of calls we've handled has doubled," says Alissa Knight, principal analyst at Alissa Knight & Associates.

This ebook will help you prepare to defend against this growing wave of attacks. It will present advice from security leaders who've protected their organizations or their clients' organizations from the three primary threat patterns attackers favor.

It will explore:

- Three most common attacks that malicious actors use.
- How organizations can defend themselves against attacks.
- Tools Tanium gives you to help defend against these attacks and whatever attacks come next.

Incoming Attacks: The Three Primary Threat Patterns

Criminals have focused most of their attacks around three primary patterns:

1. Ransomware attacks
2. Opportunistic attacks
3. Social engineering attacks

> *"There has been a significant uptick in human-operated ransomware. These are full-blown network intrusions where the bad guys can be in your network for weeks or months before they strike."*
>
> Kris McConkey, Cyber-Threat Operations Lead, PwC

Ransomware Attacks

Cybercriminals are employing a new, more complex, more dangerous form of ransomware.

"There has been a significant uptick in human-operated ransomware," explains Kris McConkey, Cyber Threat Operations Lead at PwC. "This isn't ransomware that infects a few systems, so you have to pay a couple hundred dollars in Bitcoin to get a decryption key. These are full-blown network intrusions where the bad guys can be in your network for weeks or months before they strike."

During that time, the cybercriminals do two things to compromise their target and increase the chances of quickly receiving a ransom. First, they learn how to lock up as many systems as possible. Second, they steal data and threaten a data leak as part of their attack, commonly with the endgame of selling the data on the dark web if the organization doesn't meet their demands.

This strategy has proven effective for criminals and very expensive for the organizations they target.

"Some of the top-end ransomware groups are regularly getting away with millions from a single victim," adds McConkey.

Opportunistic Attacks

Cybercriminals are also deploying less focused, more distributed attacks.

"Cybercriminals aren't always targeting your company specifically," notes Michael Coates, Co-Founder and CEO at Altitude Networks. "They're using automated attack systems to constantly scour the web and find vulnerable assets."

When they find one, they'll exploit it and compromise the organization it belongs to, no matter what that organization is or whether it's a conventional target.

"Most people used to rely on the notion of 'Why would they come after my business when there are so many other targets available?'" Coates elaborates. "But it's no longer a matter of whether they target you. It's whether they find your vulnerabilities."

Social Engineering Attacks

Cybercriminals are directly targeting work-from-home (WFH) employees who are isolated from their colleagues.

"What adversaries are doing is called 'hacking the human,' or 'social engineering,' where they target an individual at a specific company based on their title," says Knight.

They're using the same social engineering attacks they always have, but with new content themes that tap into information people have been looking for during the pandemic.

I've seen a huge surge in phishing emails, spear phishing emails, and smishing texts, all are similar scams as before, but now with a pandemic flavor to them," says Radcliffe.

While the attacks have remained the same, employees now work under very different circumstances than they're accustomed to. They're isolated and vulnerable.

"There has been an uptick of people falling for these schemes and clicking on these links and doing all the things we wouldn't normally do," Radcliffe points out.

All these threats are sophisticated and effective. To protect themselves, organizations must develop an equally sophisticated and effective range of defenses.

Advice From Security Leaders

To produce this eBook, we spoke with numerous security leaders. All have defended their own organization or their clients' organizations against this new wave of attacks, and all provide similar advice on how to defend your organization against today's threats.

Defending Against Ransomware Attacks

To defend against ransomware, organizations must focus on developing two capabilities: endpoint visibility and control.

"Organizations can only rapidly respond to a ransomware incident, investigate what happened, and take action to resolve it if they have good endpoint visibility and control," says McConkey.

Good endpoint visibility and control gives an organization a better chance to counter an attacker that tries to lock their systems, steal data, or demand a ransom.

"The decision to enter into negotiations with threat groups comes down to several factors," McConkey makes clear. "Do you have enough visibility into your IT environment to know what the bad guys touched and whether they still have a foothold? Based on the control you have, how confidently can you kick them out and keep them out?"

Organizations must develop this visibility and control before the ransomware attack occurs. And they must test how well their visibility and control holds up during an incident.

"Knowing how much visibility you have, knowing how you can react if an intruder gets in, and knowing you'll be able to kick them out of the network and batten down the hatches, is all becoming a significant focus for most organizations and their security planning," says McConkey.

"Organizations need to think about how to stress test their response systems in this new world," says McConkey. "We have new and very extreme threat categories that exert pressures organizations aren't used to coping with. Making sure you understand where the pitfalls are and how to quickly bounce back from them is very important."

> *"Knowing how much visibility you have and how you can react if an intruder gets in, and knowing you'll be able to kick them out and batten down the hatches, is becoming a significant focus of security planning."*
>
> Kris McConkey, Cyber-Threat Operations Lead, PwC

Defending Against Opportunistic Attacks

To defend against opportunistic attacks, organizations must use their visibility and control to establish and maintain fundamental IT hygiene over their remote networks. They must use their visibility to find "unknown" endpoints.

"The biggest threat to organizations today is not knowing what assets they have," warns Knight. "We refer to this as the Shadow IT problem, where an employee has deployed a server in the network that's unpatched, unsecured, and unhardened and is accessible from the internet."

And Shadow IT has only grown with the move to WFH. A former hacker, Knight understands how vulnerable these unknown assets are to opportunistic attacks and how often they create a backdoor into organizations.

"Organizations now have assets everywhere, and they have more and more devices that historically weren't connected and are now connected to their infrastructure," says Knight.

"Over the last two decades, I've hacked over a hundred networks," adds Knight. "In more than half of those compromises, I gained access to the network through an asset the company didn't know it had."

Once an organization knows what endpoints it has, it must develop enough control to close any vulnerability that an attack might find and exploit. Attackers commonly exploit very simple, preventable vulnerabilities.

"Too many breaches are the result of an attacker exploiting a vulnerability that has a patch available," explains Knight. "Organizations don't patch fast enough."

Defending Against Social Engineering Attacks

To defend against social engineering attacks, organizations must educate and train their people. They must also build defenses that secure their users in those moments when education and training fail.

Effective education and training begin with making sure employees understand what a threat looks like. They must know to look for common red flags, such as someone asking for too much information, talking about money, or trying to rush them into a decision.

Staff must also know who to speak with if they see a red flag or if they fall for a social engineering attack, clicking a link or opening an attachment that only seems suspicious after the fact. And they should know how to reach the security team working to defend them when they're no longer in physical proximity.

It's important for employees to know they won't be blamed or put their jobs at risk if a security incident occurs because of them. Blaming only makes it less likely that they'll report any social engineering attacks they encounter or trigger.

Moreover, education and training are only one layer of defense against social engineering. Even the best trained employee can fall prey to an attack. So, organizations must have additional layers of defense.

> *"Users are trying to do their jobs. Security must defend them, regardless of whether they do the right thing. Organizations need multiple layers of control to compensate when someone makes a mistake."*
>
> Michael Coates, CEO, Altitude Networks

"Users are trying to do their jobs. Security must defend them, regardless of whether they do the right thing," explains Coates. Organizations need multiple layers of control to compensate when someone makes a mistake."

Keeping in mind that there's no silver bullet, an organization can still develop effective defenses against ransomware, opportunistic, and social engineering attacks quickly and efficiently.

Five Steps to Stopping These Threats

To defend against today's biggest threats, you must develop comprehensive visibility and control over your endpoints, close as many known vulnerabilities as possible and extend user security beyond education and training. We've created a simple five-step process to help you develop these capabilities:

Step One: Assess security gaps.

Step Two: Close gaps in endpoint visibility and control.

Step Three: Close gaps in IT hygiene.

Step Four: Close gaps in user security.

Step Five: Re-evaluate endpoint management and security tools.

Step One: Assess Security Gaps

Ask yourself a few questions to identify any fundamental gaps in your security posture and determine how well you could defend against today's complex attacks:

- ✓ Do we have comprehensive visibility into our endpoints and their vulnerabilities?
- ✓ Does that visibility extend to remote devices provisioned directly by our users?
- ✓ Can we remotely apply controls like patches and updates to our endpoints?
- ✓ How long do vulnerabilities linger in our network before we close them?
- ✓ Have we updated our security policies and educated and trained our staff on them?
- ✓ How fast can we detect and resolve incidents caused by staff making mistakes?

Step Two: Close Gaps in Endpoint Visibility and Control

Review answers from step one, make a list of gaps in your security posture, and prioritize filling those gaps in your endpoint visibility and control capabilities.

Even if you don't have huge gaps, take time to ensure you've developed these capabilities to a mature degree.

Ralph Loura, CIO at Lumentum, provides a practical guideline for how mature your endpoint visibility and control must be to effectively defend yourself against modern threats.

"Having good endpoint-edge intelligence is the key to everything else. I need intelligence coming off every device, all the time. What's occurring on it — normal and abnormal— and what may or may not have been deployed," explains Loura. "That's information I can use to make better decisions about how to proceed."

> *"Having good endpoint-edge intelligence is the key to everything else."*
>
> Ralph Loura, CIO, Lumentum

To deploy mature endpoint control, you must meet these criteria.

"I must be able to touch every device on a moment's notice," adds Loura. "When threats land they can move very quickly. Responding, isolating and recovering quickly can prevent a minor issue from becoming a major issue."

If you can't meet or exceed these criteria, determine what you must do to upgrade your capabilities. And do it.

Step Three: Close Gaps in IT Hygiene

Once you confirm or develop mature endpoint visibility and control, you must use these capabilities to establish and maintain pristine IT hygiene.

"It's so critical to button up each and every issue that put you, your workplace and your data at risk," says Coates.

Establishing and maintaining IT hygiene doesn't have to be complicated. For many organizations, the first step is simply to see the link between operations and security.

"When we start talking about security, it doesn't always feel relevant to talk about operations," says Stephanie Aceves, Director of Technical Account Management at Tanium. "Things like making sure you're updating all your systems and you have a regular patch cadence."

> *"When we start talking about security, it doesn't always feel relevant to talk about operations. Things like making sure you're updating all your systems and you have a regular patch cadence."*
>
> Stephanie Aceves, Director of Technical Management, Tanium

From there, they must consistently perform the fundamentals of patching their systems, updating their applications and configuring their devices properly. And they must do it for every asset in the environment.

"I talk with CISOs and CIOs who say, 'I have 84% of my workforce's machines patched,' or, '92% of my devices are in-line with company policy," notes Chris Hodson, Tanium CISO. "Unfortunately, it only takes one weak point to be compromised, which a cybercriminal can then use as a vector to move laterally and propagate across an organization."

Step Four: Close Gaps in User Security

Ensure your staff has adequate security training and education.

"To secure remote workers against social engineering, you require education, training, and clear lines of communication, and you must eliminate blame to encourage reporting," says Radcliffe.

Even more important, build security controls that extend beyond training and keep users safe when they inevitably forget that training and make a mistake. Build layers of authentication and defense around your staff to rapidly detect incidents they've caused and limit potential damage. These additional layers of defense include:

- **User behavior monitoring** to set a baseline for normal behavior, only intervening when you notice a significant aberration.
- **Data risk and privacy monitoring** to find the instances of sensitive data and files that users have proliferated.
- **Impact analysis** to map and mitigate potential damage that any user might cause if credentials are compromised.
- **Zero trust** to add identity inspection and authentication touchpoints that raise the barrier to entry into your environment.

Step Five: Re-Evaluate Your Endpoint Management and Security Tools

Finally, determine which tools can help defend your organization against this new wave of attacks and which might have only been effective against legacy threats.

Against an escalating volume of sophisticated attacks and a larger, more complex network porous with potential vulnerabilities, you can't get by with a large suite of slow, clunky, isolated endpoint tools.

"To find and resolve issues, organizations need more efficient systems to reduce the scale of effort required by incident response teams," emphasizes Coates.

There's no need to complicate this final step. Simply take a look at your endpoint management and security tools, and ask yourself:

- Is this an isolated, single-function point solution?
- Does this require intensive manual labor to operate?
- In 2020, did this lose some or all of its ability to provide visibility and control?

Consider replacing a tool that receives any “yes” answers.

If you suffer one of the threats we’ve outlined, any isolated manual tool that delivers limited visibility and control will slow you down, burden your teams and increase the chance you’ll be unable to resolve the incident satisfactorily.

“If you have thousands or tens of thousands of devices, your team can’t manually address each of these issues,” says Loura. “You need a well-instrumented platform that can run data collection, execution, and action on a wide range of devices across the globe. An effective endpoint management solution is really key.”

An effective endpoint solution like Tanium.

How Tanium Can Protect You From Modern Attacks

We built Tanium to help defend modern organizations against modern threats, and over the past year a diverse range of organizations and security leaders have used Tanium to protect themselves and their clients from ransomware, opportunistic attacks and social engineering.

They used Tanium to maintain effective security over their networks, even as those networks rapidly evolved to accommodate the nearly overnight move to remote operations. By utilizing Tanium’s distributed architecture and edge-computing features, these leaders were able to maintain visibility, control and incident response capabilities over their endpoints.

Tanium helps organizations maintain effective defenses by:

- Delivering real-time visibility and comprehensive control over expansive endpoint environments, making it easy to raise the barrier to entry into organizational networks and perform rapid and comprehensive incident investigation, response, and attacker eviction.
- Streamlining and automating many of the core tasks of endpoint security and management, making it possible to efficiently remediate complex threats in moments when a security team feels overwhelmed by an escalating volume of attacks.
- Providing a unified platform for all core endpoint management and security capabilities, which allows security leaders to raise efficient, effective defenses without unnecessary complexity, cost, or management challenges.
- Deploying new endpoint management and security capabilities in hours or days — not weeks or months — and help technology leaders rapidly fill gaps in the security posture of their asset environments or create a comprehensive posture from scratch.

The Tanium Platform provides key services for battling today’s most dangerous cyberattacks

Asset Discovery and Inventory
Know what endpoints and applications are in the environment — even as the environment rapidly floods with new managed and unmanaged home-based agents.

Patch, Software and Configuration Management
Apply large-scale patches, software updates, installations, and policy configurations to countless distributed endpoints quickly, efficiently and with closed-loop verification.

Incident Response
Perform continuous, automated threat detection across the endpoint environment, and investigate, contain and remediate incidents found in real time.

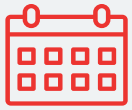
Be Ready for Whatever Comes Next

Today you must defend against the three attacks we've examined, but tomorrow you could face an entirely novel attack pattern. As your threat landscape evolves, you must find a way to keep your organization safe — no matter what vulnerabilities you have or how attackers try to exploit them.

Tanium can help you do just that.

Tanium can help fill any gaps that remain in your security posture. It can provide an effective defense against today's most common attacks and give you a modern, flexible, extensible approach to security that can rapidly adapt to whatever tomorrow might bring.

Reach out today and learn if Tanium can help secure your organization against its biggest threats. Take the appropriate next step to see if Tanium is the right security platform for you.



Schedule a free consultation and demo of Tanium.

Schedule Now

Let Tanium perform a thorough gap assessment of your current capabilities.

Get Gap Assessment

Launch Tanium with our cloud-based offering, Tanium as a Service.

Try Now

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.