TANIUM

Zero trust

The perfect solution to the perfect security storm.

We're experiencing a classic example of the perfect storm, a perfect confluence of multiple events coming together to require the adoption of a zero-trust approach to cybersecurity:

The rise of hybrid and remote work

The ongoing shift to cloud services

The continuing growth of mobile devices in the workplace

An onslaught of sophisticated attacks that can impact entire supply chains

Never have organizations faced so many challenges in protecting their data resources, and never have they needed to be more suspicious of users and devices trying to access their networks. The zero-trust model, with its principal concept that users, devices, applications and even networks should not be trusted by default, even if they are connected to a permissioned network and even if they were previously verified, is well suited to today's typical IT environment.

As cybersecurity and IT leaders know all too well, the complexities of security have increased significantly in recent years. Not only are attacks getting increasingly sophisticated, but cybercriminals are more organized than in the past, and in some cases, well-financed by nation-states.

In addition, the attack vector has broadened considerably in recent years. Hybrid and remote work models mean more people are working remotely, and in many cases, they are using their own devices and networks to access critical business data.

Furthermore, the use of cloud services and multi-cloud strategies continues to increase. Sometimes cloud deployments are not even on the radar of central IT and therefore not managed as other IT assets might be. The concept of perimeter defense has been obliterated by the rise of cloud services, remote work, and mobile environments. There is no such thing as a perimeter, or perimeter defense, anymore.

All of these developments provide good reasons for organizations to shift to a zero-trust model of cybersecurity. The idea of zero trust is fairly simple: trust no user or device, and always verify.

Unacceptable risk

There is simply too much risk that an outside entity trying to gain access actually has nefarious intent. There is too much at stake to trust anyone or anything. One of the more notable effects of the shift to zero trust is the realization that traditional virtual private networks (VPNs) are no longer fully capable of securing remote access to corporate networks.

The distributed workforce at an organization might have access to highly regulated customer data through on-premises or cloud-based customer relationship management and enterprise resource planning systems. They might also need to access commercially sensitive intellectual property — all of this from personal devices.

Organizations need an effective way to secure and authenticate these users, and unfortunately, traditional VPNs have struggled to keep up with the traffic workloads that work-from-home generates.

By combining the principle of least privilege with a modern approach of contextual access, multi-factor authentication (MFA) and network access, organizations can maintain a more agile security model that is well suited for a cloud-heavy and mobile-centric environment.

The result of the zero-trust approach is that organizations can reduce their attack surface and ensure that sensitive data can only be accessed by those users that need it under approved, validated context. This serves to greatly reduce risk.

Traditional zero trust practices have typically focused on network access and identity and access management (IAM) through single sign-on (SSO). With remote work now encompassing such a large portion of end-user access, however, device posture is increasingly important as devices act as the new perimeter in a perimeter-less world.

By adding device validation to their security protocol, enterprises can defend against criminals who steal credentials or devices and use them along with MFA to gain access to networks and data.

If a network environment is monitored for noncompliance or critical vulnerabilities, then securing the device is the last defense to having compromised sensitive data. This is why it's vital to adopt a converged endpoint management solution as part of the zero-trust approach.

Concerning VPNs

Research by Tanium has found that overtaxed VPNs were the second-biggest security challenge for organizations transitioning to a distributed workforce. The problems with legacy VPNs have not only imperiled the security of traffic flows but are contributing to a growing risk of security threats related to endpoints.

When the pandemic hit and organizations were forced to allow many employees to work from home, they relied on VPNs to support their distributed workforces, but with less than stellar results. While VPNs are familiar to many users and already in use for remote access, they are not the ideal tools to provide secure access for so many users relying on devices that, in many cases, are not as secure as they could be.

VPNs will not provide adequate defense against threats aimed at the home networks many users rely on when working remotely. In addition, the sheer number of VPNs a company might need to support an enormous mobile or hybrid workforce means the management and maintenance burdens could be overwhelming.

Zeroing in on zero trust

To truly provide secure access for a large number of remote workers, organizations need to think beyond VPNs and fully adopt the zero-trust model of cybersecurity.

With a zero-trust strategy and tools, it's easier for security teams to provide secure access to applications because they have more granular access controls, and users do not get blanket permissions. Access rights are very specific and require continuous verification.

The term "zero trust" is used a lot in the cybersecurity market and can mean different things to different people. If done right, this approach should look at three things:

1. A user's credentials
2. The data that the user is trying to access
3. The device (the endpoint) the user is employing to gain access

By combining the principle of least privilege with a modern approach leveraging contextual access, multi-factor authentication (MFA) and network access, enterprises can maintain a more agile security model that works well with a remote workforce and cloud-heavy environment.

They can reduce the attack surface and make sure sensitive data is only accessible by users who need it under approved, validated context. This serves to reduce risk.

Device validation is one of the keys to a successful zero trust strategy, and with remote work making up a large portion of end-user access today, device posture is extremely important. Devices, in many cases, are the new "perimeter" within organizations, and device validation enables organizations to protect against stolen credentials or even stolen devices that cybercriminals can use to gain access to networks.

This is why practicing strong endpoint management is such an important part of a zero-trust approach. Without real-time and accurate endpoint management, organizations can't enforce compliance or validate device posture as a prerequisite for access. Authentication alone can't ensure that a device is secured.

The right tool can allow security teams to continuously check device posture against policies, to ensure that the zero-trust approach really does trust no one, even after identity and access policies are in place. Ideally, organizations should be able to integrate new zero-trust solutions with the tools they already use, so they don't have to start from scratch.

The key components of a zero-trust practice should include:

Device compliance monitoring and enforcement to confirm security posture for the device and give security teams the ability to take action if something is not right.

Identity and access management, to authenticate users' identities and compare their access against role-based rules.

Network access controls, including restricting access to resources network segments based on a user's persona and the device being used.

“Better safe than sorry” is not negative

The concept of zero trust might come across as negative — even paranoid: Don’t trust anything, whether it’s devices and other endpoints, applications, networks or individuals. But what the model really indicates is that organizations are operating in uniquely challenging times, and much is at stake when a data breach or ransomware attack occurs.

More people are working remotely, in many cases using their own devices and networks. Companies are relying on cloud services more than ever. Attacks have become more sophisticated and can **impact entire supply chains.**

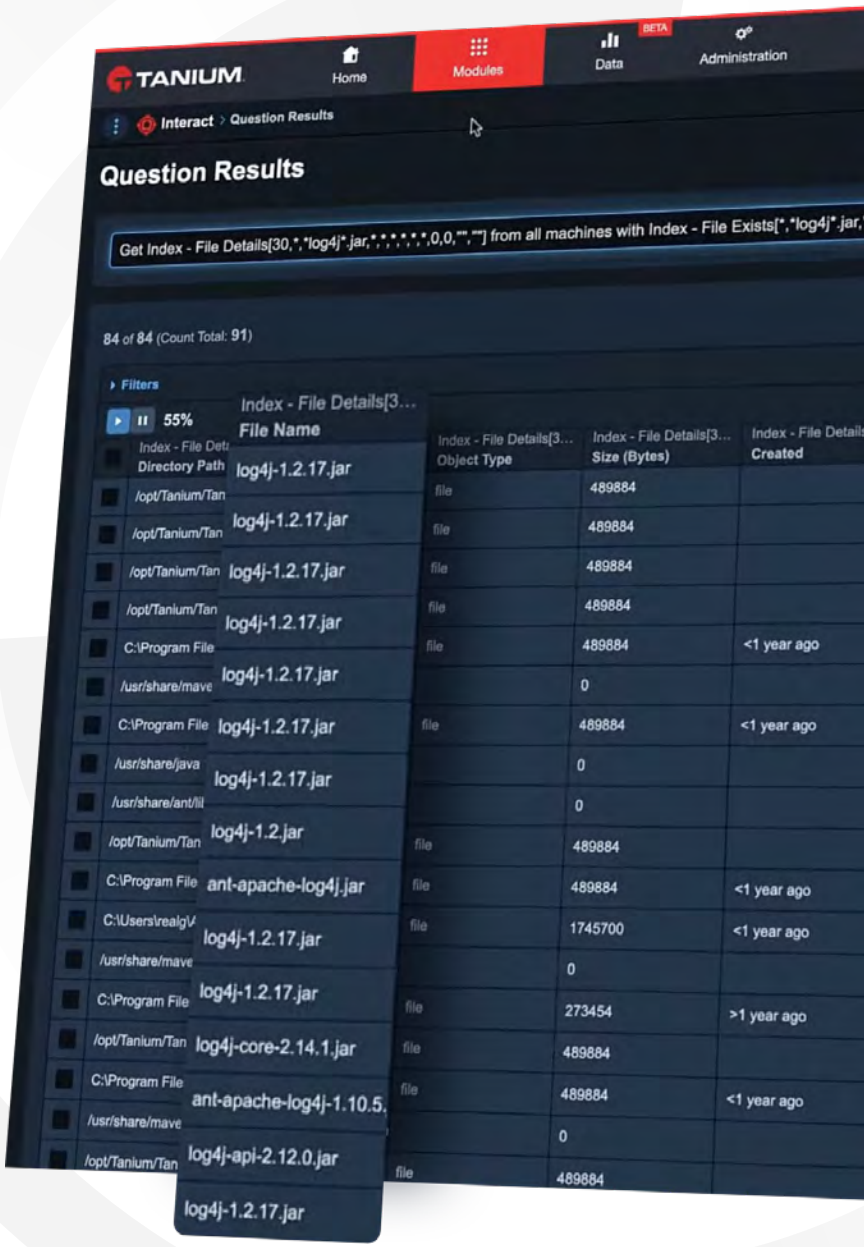
Organizations need to take the initiative to ensure that valuable data resources are always protected and to be certain that the users and devices trying to access their networks will not do harm. Implementing a **zero-trust strategy** is a truly effective way to achieve this level of security.

Perfect example of the perfect storm – Log4j

The discovery of the **Log4j vulnerability** in December 2021 is one of the more recent, and prominent, reminders of why cybersecurity teams need to implement a zero-trust security architecture.

Not that they should need reminders. Incidents are happening every day, and some of them — such as ransomware attacks that impact virtually entire supply chains — make a lot of headlines. In the case of Log4j, a Java-based logging utility that's part of the Apache Logging Services, security researchers found a zero-day security vulnerability involving arbitrary code execution.

This was no garden variety vulnerability. Security experts described the flaw as being one of the biggest and most critical discoveries in recent years. And it provides a glaring example of how at-risk organizations can be. New software vulnerabilities are being uncovered all the time, and some of them can lead to serious security breaches and lost data.



Security fundamentals

Along with deploying the zero-trust approach, organizations should be sure to pay heed to security fundamentals. For example, they need to patch vulnerabilities as soon as they are identified. The Log4j development showed why that is important.

Patches should be installed and updated, but not in a haphazard way. Comprehensive patch-management programs should encompass all devices used in the organization that are connected to the internet and corporate networks.

Another good practice is to reassess all endpoints where systems are vulnerable to attacks. This includes conducting an audit of all those systems and devices that have administrative access to network systems, and an evaluation of the security protections on any sensors or other internet of things (IoT) devices tied to networks.

On a longer-term basis, companies need to reassess how they gather, store and categorize the growing volumes of data they are managing. That might mean segmenting data so that more stringent security controls are placed on access to the most sensitive data — such as personal information or intellectual property.

In addition, organizations need to be vigilant about using MFA and strong passwords. Networks have been compromised because hackers guessed users' passwords, which suggests a need for policies that require more complex passwords or the use of MFA.

Users can be careless when it comes to cybersecurity practices, so providing good training programs and running awareness campaigns are also good ideas to educate everyone in the organization. These programs should cover signs to look for that indicate phishing and other attacks, as well as social engineering techniques frequently used by bad actors to gain sensitive information or network access.

By deploying a zero-trust model and taking care of the cybersecurity "basics," organizations can put themselves in a position to defend against the latest threats, including ransomware.

Security today requires more than simply managing identities and authenticating users. It needs to assume that anyone or anything trying to get into the network is an intruder — until proven otherwise.

Next steps

Learn how Tanium's Converged Endpoint Management (XEM) platform can support a robust zero-trust practice.

Learn more

Tanium, the industry's only provider of Converged Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

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