TANIUM™

Tanium Insights: It's Time to Ditch the VPN for Zero Trust

Zero trust was made for this new era of cloud and remote working. Learn how a zero-trust model can remove the security bottleneck of the VPN while minimizing cyber risk and supporting user productivity.

Introduction

What is the essence of zero trust? Just what the name implies. Don't trust anything. No individual. No endpoint. No application. No network.

Enterprises must recognize they operate in a hostile environment. Zero-trust security assumes no device or user can be trusted without verification.

Organizations should not automatically trust anything inside or outside their perimeters. In fact, the idea of a perimeter — the castle-and-moat approach to security — is long past its "use by" date.

The zero-trust framework was created in 2010 by John Kindervag, who at the time was a principal analyst at Forrester Research Inc. It's been gaining traction in the security marketplace for a decade. But in 2020, the nearly overnight transition to a distributed workforce driven by the COVID-19 pandemic has dramatically increased interest in zero trust.

Why? Well, your distributed workforce might have access to highly regulated customer data via corporate and cloud-based CRM and ERP systems. And they might regularly need to access commercially sensitive intellectual property from their home PCs and devices. Organizations need an effective way to secure and authenticate these users.

Unfortunately, traditional virtual private networks (VPNs) have struggled to keep up with the traffic workloads that work-from-home (WFH) imposes.

Tanium research found that overtaxed VPNs were the number-two security challenge for organizations transitioning to a distributed workforce.

These problems have not only imperiled the security of traffic flows but are now contributing to a growing powder keg of security dangers related to endpoints. A quarter (26 percent) of CXOs polled said they de-prioritized patching altogether in the first few months of the pandemic.

This approach, while understandable, means that more and more endpoints are not up-to-date and protected against cyberattacks.

And this "powder keg" has an actual cost. As reported by McAfee, cybercrime now costs the world economy more than $1 trillion, or just more than one percent of global GDP, which is up more than 50 percent from a 2018 study that put global losses at close to $600 billion.

In this white paper, we examine what kick-started the zero-trust movement, why it's completely changed the conversation around network security, how Tanium and its partners' capabilities contribute to a zero-trust solution.

We also cover what you need to know about adopting zero trust in your organization. Hint: You don't get up one morning and decide to adopt zero trust.

History of Zero Trust

Although Forrester Consulting gets the credit for bringing the terminology of zero trust into the mainstream, the real beginning of zero trust was the "breach heard round the world." And that breach occurred in 2010, when highly sophisticated hackers originating from China targeted Google's corporate infrastructure and, using layers of encryption and multiple malware programs, managed to steal intellectual property.

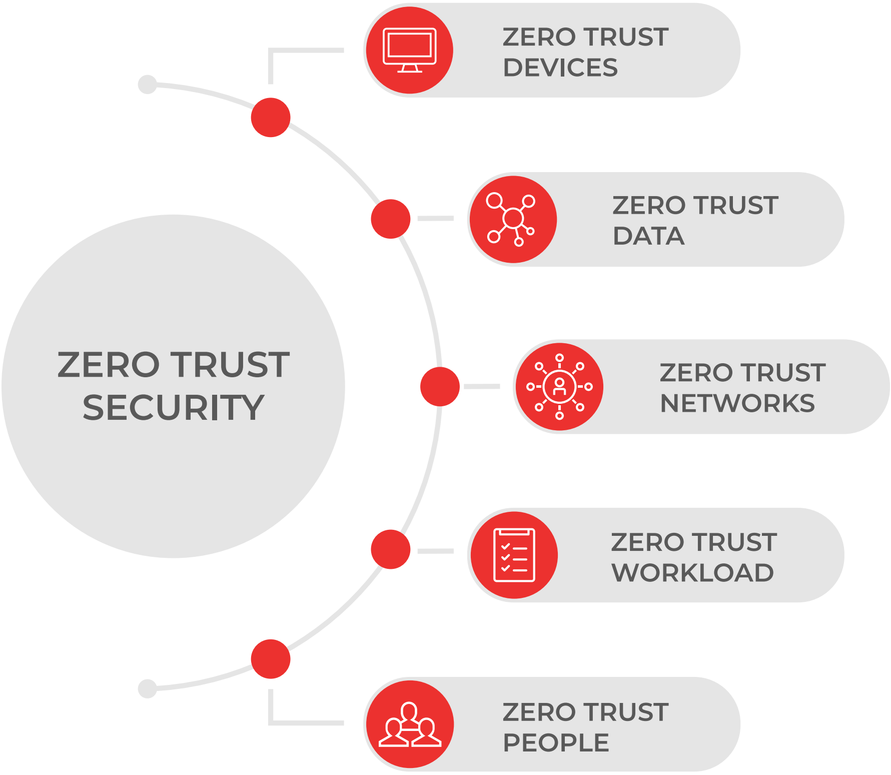
Google's response was to completely redesign its network structure. The company wrote a paper called BeyondCorp, about a futuristic company that jettisoned traditional security concepts and re-architected its network in the image of what we know today as zero trust. This is where Forrester got the idea, coined the term and created a market for zero-trust solutions.

As more and more organizations moved traditional on-premises workloads to the cloud, they looked to Google to help with security. They kept asking about BeyondCorp. So, as Google formed the Google Cloud Platform (GCP) business unit and continued to add products and features to the platform, it made BeyondCorp a product.

BeyondCorp is not a single technology, a silver bullet that solves all security problems, but it's opened the door for companies to begin the journey to zero trust.

IT Teams Need to Rethink Their Network Security Strategies

As we mentioned earlier, when the pandemic struck, organizations fell back on VPNs to support their distributed workforces — with less than stellar results. But VPNs were familiar and already in use. They weren't the best tool for the job, but then what was?



Anton Chuvakin, head of security solution strategy at Google Cloud, doesn't like VPNs much. "They break," he explains in a recent interview with Endpoint. "A lot. And at the worst times." "VPNs are great if maintained and configured correctly," he continues, "but they don't protect against threats carried in through a home network."

The hassles of using VPNs and the security issues they present to the remote workforce are very much on Chuvakin's mind, as are the other challenges enterprise technology faced last year. With workers suddenly beyond their firewalls, security teams raced to safeguard them with the anti-malware software and monitoring systems the office network once provided.

As remote work evolves into the world's new normal, these teams must now ensure that authentication is informed, secure and easy to use across the entire enterprise.

Many must do this across complex hybrid cloud environments or struggle with legacy systems and old applications. That's why now is a good time for zero trust. Zero trust is a more straightforward answer to the remote-access problem than VPNs.

According to Chuvakin, zero trust is one of those rare cases where you can have a balance of easy yet secure. In the past, if you needed direct network access, you'd use the VPN, and once you were in, you were in, and you could access many things, which increases risk.

Today, in the world of browser apps and API [application programming interface] access, it's a lot easier for security teams to provide secure access to these applications and for employees to access these applications.

It's more secure because you get more granular access controls, and people don't get blanket permissions; permissions are very specific. It's easy because users don't have to think about launching a VPN client or configure digital certificates. That's all taken care of.

The Endpoint Is the New Perimeter

You'll hear many analysts say identity is the new perimeter. And that's great until you ask the question — and COVID-19 dramatically highlighted this — what if a user is accessing the corporate network from a personal computer at home that hasn't been patched in four years? What if that endpoint has been compromised?

It now has access to a company's product development data, possibly its code repository, and its customers' credit card information. The user was validated, but what about the device and the software on it?

> “This stuff is really hard. That's the recurring theme with a lot of the customers I encounter. But, ultimately, they have to transition to this model. If they don't, it's very likely that all the IT layers, with all the individual authentication access methods, would crash on them.
>
> You need to have these high-risk environments done the modern way, through zero trust. It's not manageable to have one VPN over here and another VPN over there. Eventually, the complexity would kill you.”

Anton Chuvakin
Head of Security Solution Strategy,
Google Cloud

This realization triggered Google's interest in the Tanium Platform. Its customers continuously ask for more intelligence at the endpoint. While Google can look at the user, it can't deeply interrogate the endpoint.

Tanium's partnership with Google and BeyondCorp gives them this intelligence. They have more data available at the endpoint at the time of user authentication to truly enforce the concept of zero trust.

"Tanium is a really good endpoint sensor, which is built not just for security, but for operations as well," Chuvakin notes. "Tanium offers a good way to collect trusted telemetry from the endpoint and channel it into authentication and monitoring decisions. Tanium is an endpoint source of truth, which zero trust relies on."

In other words, Tanium brings the perspective of the endpoint to zero trust. Identity isn't the new perimeter; the endpoint is the new perimeter. Until very recently, the endpoint perspective has been the missing piece in the zero-trust model.

Zero-trust security requires users to prove who they say they are with multi-factor authentication (MFA). Once identified and verified, users are then provided access only to the specific resources they need. A zero-trust model also applies micro-segmentation to break a network into smaller security zones, restricting lateral movement.

This is all great, but without endpoint visibility, devices at the network edge can remain critically exposed to threats via unpatched vulnerabilities and insecure configuration settings. Alongside user authentication, organizations must have the means to check endpoint "identity" by confirming the security status of remote machines.

Adopting a Zero-Trust Model

Last year, Google assembled a group of partners that shared its zero-trust vision to create the BeyondCorp Alliance. In April 2020, Google announced BeyondCorp Remote Access: its first commercial product based on the zero-trust approach.

The company introduced a second BeyondCorp zero-trust product on January 27, 2021, with additional enterprise capabilities and an expanded partner ecosystem that includes Tanium.

These partners allow BeyondCorp customers to employ existing controls to make zero-trust adoption easier while adding key functionality and intelligence, such as contextual access to the highest-value data, supporting better security decision-making.

For example, a zero-trust best practice would be having much more robust controls for an endpoint that regularly accesses business-critical information than for one that is routinely accessing company email.

In fact, for the highest-priority data, an endpoint might be restricted to that data alone. This is just an updated approach to tiered access controls, which have been an accepted security practice since the early 1990s.

Like any large IT initiative, you need to move toward a zero-trust methodology gradually, prioritizing the applications you address first. No one wakes up and says, “We’re going to implement zero trust today.” Companies that have been around for decades have thousands of servers running internal applications in their data centers.

For example, an insurance company in the Midwest may have a very complex IT environment with some really old tech. Entirely re-architecting this via a zero-trust model is an enormous undertaking.

Can zero-trust access work there? Yes, and the motivation to do it is vital because the pyramid of complexity and layers of authentication they’re trying to maintain will eventually bury them.

Key Takeaways

What is the essence of zero trust? Don’t trust anything. No individual. No endpoint. No application. No network. Enterprises must recognize they operate in a hostile environment.

As remote work evolves into the world’s new normal, security teams must ensure that authentication is informed, secure and easy to use across the entire enterprise.

VPNs break a lot, and at the worst times, and they don’t protect against threats carried in through a home network.

The endpoint is the new perimeter. Tanium brings the perspective of the endpoint to zero trust.

Zero trust began with a breach in 2010 when highly sophisticated hackers originating from China successfully targeted Google’s corporate infrastructure. As a result, Google entirely redesigned its network structure.

Google partners like Tanium allow BeyondCorp customers to employ existing controls to make zero-trust adoption easier while adding key functionality and intelligence.

Move toward a zero-trust methodology gradually, prioritizing the applications you address first.

Don’t do the hardest thing first.

> The best advice: don’t do the hardest thing first. With BeyondCorp, organizations can avoid this by starting small and moving to bigger projects as their understanding of zero trust matures.

It’s also worth remembering Chuvakin’s comments: “Organizations often say to us: ‘Well, you guys have this amazing system that works well. It’s buttery smooth. It’s secure. It gives you all the telemetry you need.’ What they forget is it took Google — with some of the best engineers on the planet — roughly 10 years to get to this buttery smooth, super-secure, super-easy system.”

Conclusion

We live in complicated times. Where once there was a clear model for network security — let the good guys in and keep the bad guys out — today, things are more complex.

To stay secure, today’s distributed businesses need to easily monitor and control all activities across the network for both users and endpoints. Organizations need a seamless security model designed for the new reality of remote work, cloud services and mobile communications.

Zero trust was made for this new reality. And the key to making zero-trust security work at scale is endpoint visibility.

By adopting a zero-trust model, organizations remove the security bottleneck of the VPN and eliminate other risks associated with the traditional approach for network security.

In the end, companies can minimize cyber risk while supporting user productivity in a new era of cloud and edge-powered remote working.

About Tanium

Tanium offers endpoint management and security that is 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 US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium has been named to the Forbes Cloud 100 list of “Top 100 Private Companies in Cloud Computing” for five consecutive years and ranks 4th on FORTUNE’s list of the “Best Workplaces in Technology 2020.” Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

TANIUM

tanium.com

@Tanium

info@tanium.com