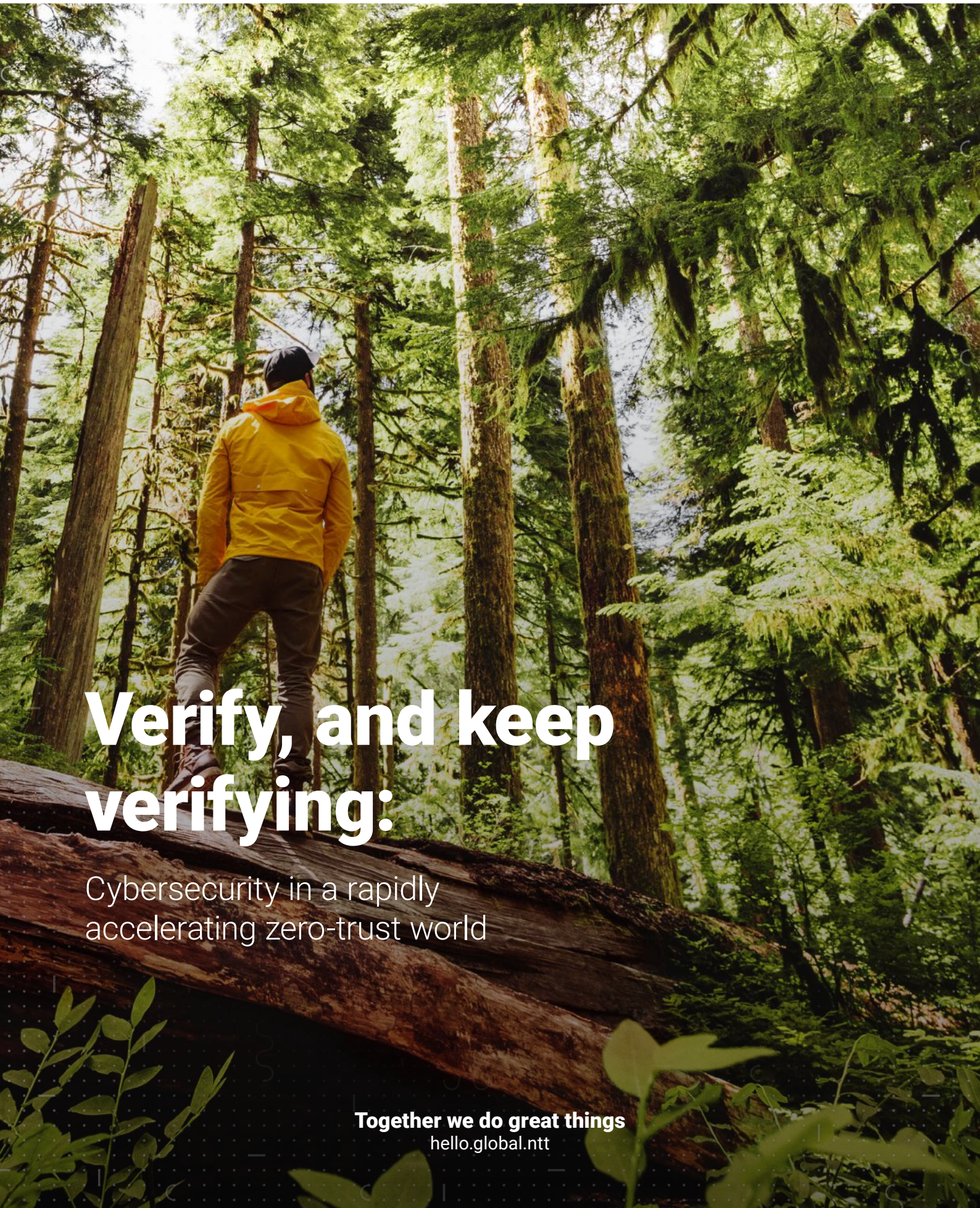
NTT | cisco

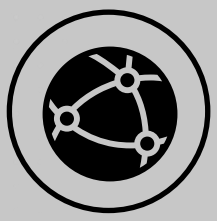
INSIGHTS
DRIVEN BY DATA



Verify, and keep verifying:

Cybersecurity in a rapidly accelerating zero-trust world

Together we do great things
hello.global.ntt



Verify, and keep verifying: Cybersecurity in a rapidly accelerating zero-trust world

In the 1980s, US President Ronald Reagan adopted a signature phrase – 'trust, but verify' the translation of a Russian proverb – in delicate negotiations with the Soviet Union, as the world was under the threat of nuclear annihilation. This was a great framework to ensure that both East and West complied with the conditions of the nuclear disarmament treaties that ushered in the end of the Cold War.

However, Reagan's approach no longer applies in the world of politics and definitely not in the world of network security. We've moved from the dichotomy of the East and West separated by the Berlin Wall, to a world where there are no longer the same clear delineations between who or what is inside and outside the enterprise network. Now, as businesses have undergone digital transformation, we have distributed working environments and user devices, web services and APIs, automation, IoT, cloud computing, and other services and connections that have completely blurred what we once thought of as the network perimeter. We need to take a zero-trust approach, no longer taking it for granted that we have a secure workplace, workload, or workforce.

Absolute security has always been an impossible goal, but we need to adopt a new framework to truly minimize business risk. We are now in a digitally transformed world that has created a completely dynamic environment where a static trusted state can never be assumed.

As a result, we need to take a 'verify, and keep verifying' approach to network security to authorize and protect your workplace, your workload, and your workforce.

Mary K. Pratt, 'What is Zero Trust? A model for more effective security', CSO Australia, 16 January 2018 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Absolute security has always been an impossible goal, but we need to adopt a new framework to truly minimize business risk. **We are now in a digitally transformed world that has created a completely dynamic environment where a static trusted state can never be assumed.**

Accelerated digital transformation

Accelerated digital transformation

Up until now, most organizations have had the luxury of moving at their own pace with developing and implementing security measures to meet the requirements of their digital transformation projects. That's all changed with the COVID-19 pandemic. We are now seeing digital transformation in weeks, not years; a rapid acceleration in the state we have been building towards with regards to a zero-trust model.

With the lockdown of communities and businesses around the world, most organizations are operating with a remote workforce and relying more on their web presence (e.g. customer portals and supported web applications); this is increasing reliance on the very systems which attackers have already been targeting. In the latest findings from NTT Ltd.'s 2020 Global Threat Intelligence Report (GTIR), application-specific (40%) and web-application (20%) attacks dominated in Australia, accounting for nearly 60% of all attacks combined[1]. It should be noted that this data was gathered in 2019, well before the impact of the COVID-19 pandemic on organizations.

Many of these attacks could still be avoided, with several old versions of malware like WannaCry and Conficker still causing damage, and known vulnerabilities remaining unpatched. According to GTIR, the most targeted vulnerability in Australia was OpenSSL (CVE-2017-3731) which has had patches available for over two years. OpenSSL was the second-most commonly attacked software technology in Australia, after attacks on Netis/Netcore and other related routers and network devices[2].

Threat actors are more likely to find these vulnerabilities because they can infiltrate environments in stealth mode by taking advantage of weak or absent continuous security verification and monitoring practices, allowing them to do more surveillance and probe more intensely without being discovered. In a zero-trust world, you need a platform approach and a cohesive vendor ecosystem to ensure you can share security information and data across the environment. That way, you can increase the level of automation, including AI and machine learning, to take away the burden of investigating the sheer scale of alerts that needed to be triaged and investigated daily. Time to detect is a critical factor in stopping threats and limiting damage to your corporate assets and systems, so visibility across the entire environment and automating the identification of anomalous behaviour and suspicious network traffic is critical for rapid investigation and action. Security controls are only as effective as the quality of the threat intelligence upon which they take action; platforms like Cisco Talos provide organization real-time threat intelligence directly into Cisco security solutions helping organizations increase efficacy and reduce time to detect.

Most analysts agree that in the new normal of the post-COVID world, to ensure greater resiliency, organizations will be enabling a more permanent remote workforce and also placing greater reliance on cloud services, automation and their own web presence, such as customer portals, retail sites, and supported web applications. As a result, they risk exposing themselves through systems and applications that cybercriminals are already targeting heavily.

With a larger and potentially more permanent remote workforce, compromised credentials will continue to be the predominant line of attack for cyber criminals. "Of all reported cyber incidents, 79% involved compromised credentials with phishing, brute-force attack, or unknown methods. In aggregate, this means that over half of ALL breaches, whether caused by a cyber incident, human error or system fault can be traced back to a credential-based issue. Compromised credentials are the single cause at the root of most breaches[3].

[1] *2020 Global Threat Intelligence Report', NTT Ltd., May 2020 https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report*

[2] *Ibid.*

[3] *Ted Kietzman, 'Lessons from Australia's "OAIC's Notifiable Data Breach Statistics Report"', Cisco's Duo Security Blog, 6 February 2020, https://duo.com/blog/lessons-from-australia-s-oaic-s-notifiable-data-breach-statistics-report*

Major security gaps emerging

Major security gaps emerging

This rapid digital transformation has increased the surface area for cyber attacks and further eroded the traditional perimeter of the enterprise network, exposing significant weaknesses as security measures struggle to keep pace with the rate of change. Everyone is moving rapidly to cloud-based services and applications, and that's where we are going to see a big shift in focus for cyber attacks and exploitation of vulnerabilities.

Phishing attacks have always exploited a constant vulnerability in organizations: human behaviour. That risk has grown exponentially with the sudden escalation in remote workers accessing the corporate services and data via their home connections. Cybercriminals prey on the latest disasters, on people's fears, doubts and uncertainties, and on topical issues of the day to lower worker's guards. Earlier this year, that was the Australian bushfires, now it's COVID-19 and in the future, it will be something else.

Since mid-January 2020, websites posing as 'official' COVID-19 information sources - but hosting exploit kits and/or malware - have been created at an incredible rate, sometimes exceeding 2000 new sites per day. We've also seen attacks spoofing or redirecting DNS, or hijacking router DNS settings via weak or default admin passwords.

We've seen several successful ransomware and crypto-jacking attacks launched from a user's device from malware inadvertently downloaded from an email attachment or via a weblink.

The issue is, how do organizations continue to ensure employee awareness and vigilance with regards to this method of attack, and also provide them with greater endpoint device management and security infrastructure to prevent this malware from gaining access to corporate systems? In Cisco's 2020 CISO Benchmark Study, more than half (52%) of the survey respondents said that mobile devices are now very or extremely challenging to defend. They've overtaken user behaviour, which was the biggest challenge from last year's report[4].

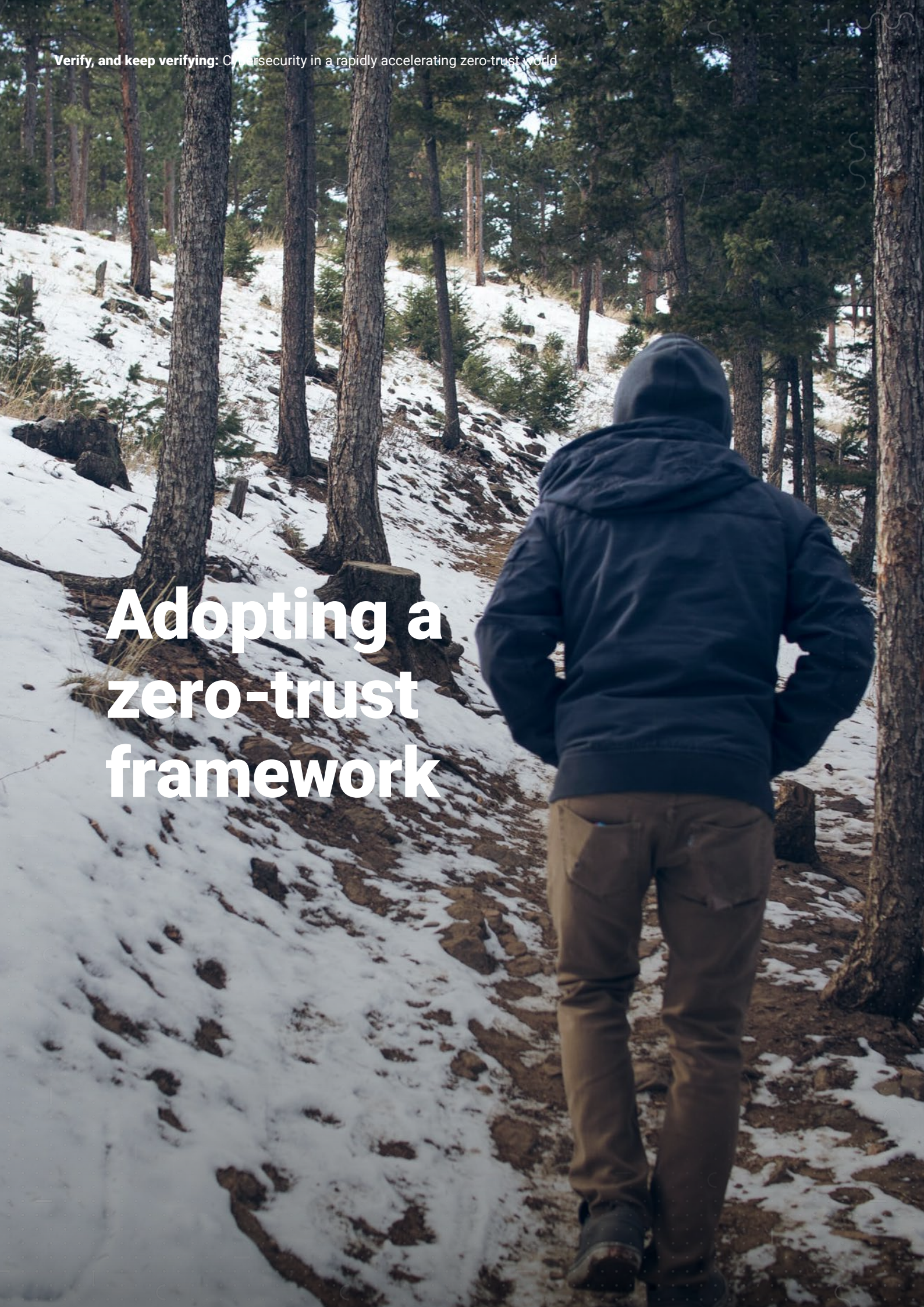
The other major problem is that without early detection and visibility or continuous verification, once the hacker has been verified and has access, we are assuming we can trust them. In this environment, sophisticated hackers have far more time to plan out a long-term approach and sequence a set of ways to breach the environment after their first attack is discovered. That's leading to second and third wave attacks that can be devastating for an organization.

This constantly shifting landscape means it is critical we apply a continuous verification approach to security.

We've seen several successful ransomware and crypto-jacking attacks launched from a **user's device from malware inadvertently downloaded from an email attachment or via a weblink.**

Cisco 2020 CISO Benchmark Report', Cisco, February 2020 https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

[4] *Cisco 2020 CISO Benchmark Report', Cisco, February 2020 https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html*



Adopting a zero-trust framework

Adopting a zero-trust framework

One of the big security advances for Ronald Reagan's USA during the Cold War came as a result of the deployment of satellites, increasing the US's ability to gather intelligence, maintain visibility and analyse the activities on other geopolitical players. Similarly, it's critical to ensure your organization has comprehensive, real-time visibility and the ability to apply context and share actionable intelligence across the entire corporate ICT environment, to best address the advanced persistent threats prevalent now and in a post-COVID world.

The good news is that, as security operations, we are moving in the right direction. In Cisco's 2020 CISO Benchmark Study, respondents were asked for their organization's investment in Identify, Protect, and Detect measures to prevent future incidents. 'Identify' saw a rise in expenditures from 21% to 27% from 2019 to 2020 while 'Protect' and 'Detect' remained constant at 25% and 18% respectively. This trend shows that organizations are spending more on prevention versus being reactive in their cybersecurity posture.

That visibility forms an important element in building a more cyber-resilient business. Cyber-resiliency is the ability of an organization to continuously deliver products and services despite cyber-related events impacting normal operations. This belief embraces the concept that security is not absolute and that businesses must prepare for, prevent, respond, and successfully recover to secure state without disruption or degradation to normal delivery expectations.

In addition to this greater visibility, and automated and managed threat intelligence, it is essential to implement infrastructure, applications, and operations that are secure by design. By adopting a zero-trust framework, you can identify and verify every person, device, and application trying to access your infrastructure.

Cisco's approach covers the spectrum of your workforce, workloads, and workplace. It incorporates a number of its key technologies into an approach that now means it's possible to meet the needs of the modern enterprise from both a security and compliance basis. It focuses on three key attributes:

enforcing policy-based control

greater visibility across your entire environment

detailed logs and reporting to help detect and respond to threats.

A zero-trust framework will ensure that you are deploying a layered defense, continually authenticating your users, managing and controlling your devices, visibility of the applications and, through segmentation, limiting where workloads can run throughout your network.

This framework comprises three key continuous verification pillars:

The user is identified and authorized using multi-factor authentication (MFA).

The device or endpoint being used is known, and compliant with security policies and standards.

The user (and any applications or workloads they are running) is limited to where they can go within your environment.

In other words, 'verify, and keep verifying'!

‘Recognizing that existing approaches aren’t doing enough, enterprise leaders are searching for something better – and are finding that the Zero Trust model can deliver the best results.

Chase Cunningham, a principal analyst at Forrester

Zero trust is a pragmatic and future-proof framework that can help bring effective security across your architecture – spanning the workforce, workload, and workplace. Having zero trust in place removes much of the guesswork in protecting your infrastructure from all potential threats, including mobile devices.

It’s important that you take a secure by design approach to your zero-trust framework, which means including security as a key and conscious deciding factor in the approach to designing end-to-end business solutions. This will result in a cyber-resilient solution and enable businesses to better cope with unprecedented and unexpected events in the future – like the situation we are in right now with COVID-19.

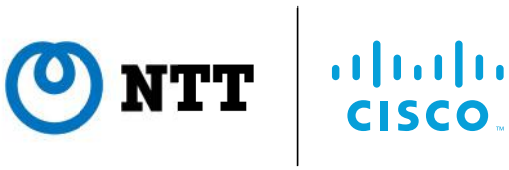
Implemented properly, cyber-resilience brings together information security, business continuity, and organizational resilience, ensuring a secure by design approach. Security best practices must be considered and built into policies, procedures, infrastructure, and applications, as well as provide appropriate visibility into, and control over these components, regardless of normal or adverse activity. It is only with this approach, within a zero-trust framework, that organizations can truly minimize business risk.

Trust is a natural human need, and it plays a fundamental role in how we interact and communicate, helping to bring an end to the Cold War with the fall of the Berlin Wall. In today’s world, we still need to create a trusted environment, but this is increasingly difficult as digital transformation accelerates at pace. To secure the fluid and dynamic environment our enterprises operate in today, we need continuous verification: so never forget to ‘verify, and keep verifying’!

It’s important that you take a secure by design approach to your zero-trust framework, which means including security as a **key and conscious deciding factor in the approach to designing end-to-end business solutions.**

Mary K. Pratt, ‘What is Zero Trust? A model for more effective security’, CSO Australia, 16 January 2018 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Zero trust is a pragmatic and future-proof framework that can help bring effective security across your architecture – spanning the workforce, workload, and workplace. **Having zero trust in place removes much of the guesswork in protecting your infrastructure from all potential threats, including mobile devices.**



We partner to deliver a connected customer experience