White Paper

HardenStance

Zero Trust Opportunities for MSPs and MSSPs

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

CYBERARK® paloalto® NETWORKS

November 2021

Executive Summary

- Although ‘Zero Trust’ is clearly critical to hardening cyber security posture, many customers need help understanding the value proposition and how it gets delivered.
- The SolarWinds and Kaseya attacks show that many MSPs are unable to abide by the first rule of medicine: ‘first, do no harm.’ Zero Trust can help them live up to it.
- Zero Trust is a comprehensive architecture and not all the required capabilities are fully mature yet. Each MSP or MSSP must carefully choose which specific customer needs to serve from its own portfolio of consulting, products and managed services.
- It isn’t critical for an MSP or MSSP to tightly couple its Zero Trust service portfolio with its own internal Zero Trust roadmap - but there are clear business benefits.

Cyber Security is a Growing Opportunity for MSPs

You can be a Managed Service Provider (MSP) providing IT products and services to small and medium businesses (SMBs), generating as little as 15% of revenues from cyber security. Or you can be a Managed Security Service Provider (MSSP) generating substantially all your revenues from cyber security, serving large and medium enterprises. Either way, available data points to a positive business outlook:

- In its’ world-wide annual ‘Top 250 MSSPs’ survey report for 2021, MSSP Alert states that average MSSP revenues will grow by 16% again in 2021, just as they did in 2020. This is a couple of points more than the 10-12% numbers cited by many analyst firms for the growth of the global cyber security market as a whole.
- In a July 2021 report, Analysys Mason predicted annual world-wide SMB spending on cyber security will increase from $57 billion in 2020 to $90 billion by 2025. It forecasts a CAGR of 14% for managed security – the highest of any market segment – taking global SMB spending on this segment to 30% of the total.

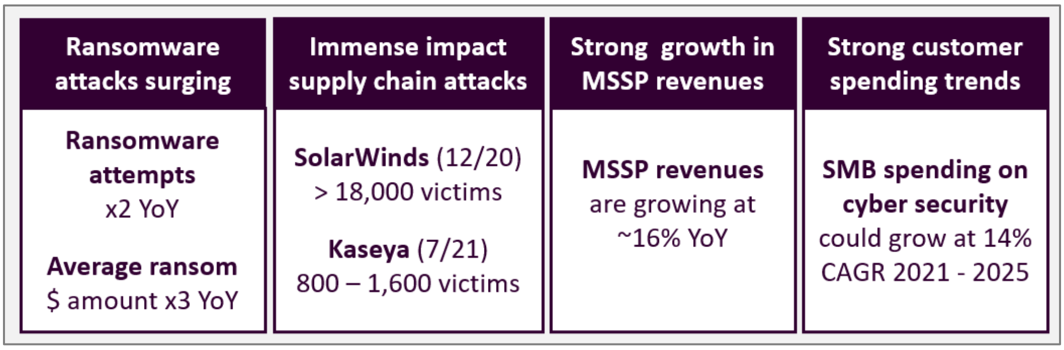
The average ransom payment increased from just over $115,000 in 2019 to $570,000 in the first half of 2021.

A Worsening Risk Outlook for Organizations and Citizens

As summarised in **Figure 1**, and discussed below, the probability of continued strong growth in demand for cyber security services is explained in part by generally worsening trends in the threat landscape and the unusually big impact of some recent breaches:

- **There has been a global surge in ransomware attacks.** SonicWall saw 304 million ransomware attempts in the first half of 2021 – as many as the whole of 2020. Palo Alto Networks’ Unit 42 research unit reports that the average ransom payment increased from $115,000 in 2019 to $570,000 for the first half of 2021. Double extortion has become a lot more common – a second ransom demand for not leaking data on top of the first for decryption keys to unlock it. With business operations even more vulnerable due to the pandemic, the healthcare sector has been viciously targeted. And in May, disruption to retail gas supplies due to a ransomware attack on Colonial Pipeline impacted millions of U.S. consumers.

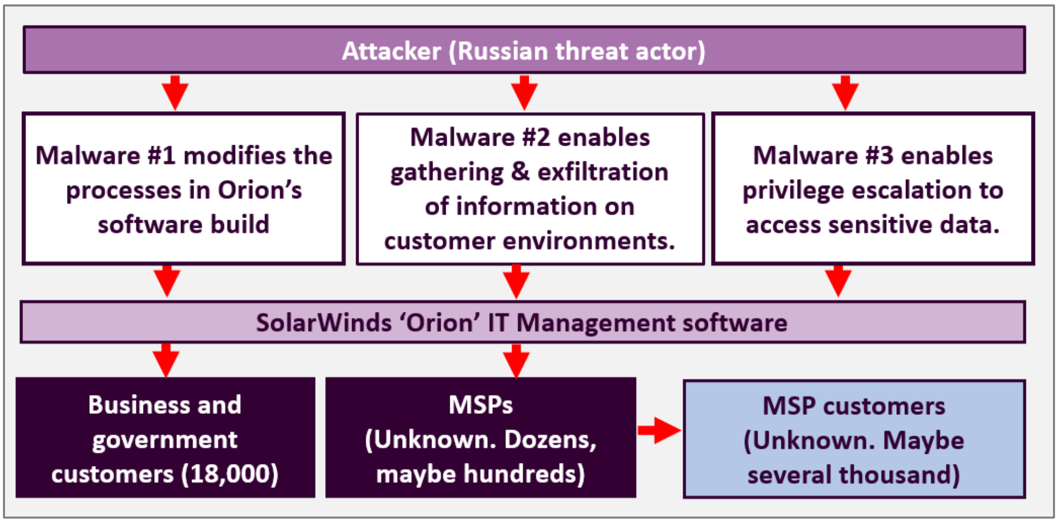
Figure 1: The State of Cyber Security in Numbers



Ransomware attacks surging	Immense impact supply chain attacks	Strong growth in MSSP revenues	Strong customer spending trends
Ransomware attempts x2 YoY **Average ransom** $ amount x3 YoY	**SolarWinds** (12/20) > 18,000 victims **Kaseya** (7/21) 800 – 1,600 victims	**MSSP revenues** are growing at ~16% YoY	**SMB spending on cyber security** could grow at 14% CAGR 2021 - 2025

Source: data from Palo Alto Networks Unit 42, MSSP Alert, Analysys Mason

Figure 2: A Simplified Anatomy of the SolarWinds Attack


Attacker (Russian threat actor)
Malware #1 modifies the processes in Orion's software build
Malware #2 enables gathering & exfiltration of information on customer environments.
Malware #3 enables privilege escalation to access sensitive data.
SolarWinds 'Orion' IT Management software
Business and government customers (18,000)
MSPs (Unknown. Dozens, maybe hundreds)
MSP customers (Unknown. Maybe several thousand)

Source: HardenStance

- **Recent supply chain attacks on IT management software providers, Solar Winds (see Figure 2) and Kaseya (see Figure 5) have enabled devastating breaches of several thousand customers.** As many as 18,000 organizations may have been impacted by the breach of SolarWinds' Orion software. Among the known victims are SolarWinds customers like Intel, Cisco and VMware, the U.S. Treasury, Commerce, State, Energy and Homeland Security departments. The Kaseya attack saw ransomware delivered to between 800 and 1,600 organizations. In both cases, MSPs figured prominently as unwitting conduits for these attacks.

It's a long-standing myth that cyber attackers are mainly interested in large organizations.

It's a long-standing myth that cyber attackers are mainly interested in large organizations. The market trends and major incidents of the last 18 months have done nothing more than accelerate the rate at which small businesses have been suffering the one-off financial costs, disruption to business operations and reputational damage inflicted by data breaches. Verizon's Data Breach Investigations Report (DBIR) captures this very well. While the 2020 edition shows small businesses suffered less than half as many breaches as large organizations, the 2021 edition shows that gap narrowing markedly with 263 breaches of small organizations identified against 307 of large ones.

As organizations continue adjusting to the operational disruption created by the pandemic, there are big opportunities for MSPs and MSSPs to support customers in capturing the benefits of digital transformation, cloud transformation, remote working and the distributed enterprise – while simultaneously adjusting their security posture to better defend against cyber risk. Most organizations have no appetite for doing all their cyber security themselves. Even if they did, the ongoing world-wide shortage of hiring and keeping skilled cyber security people remains cost-prohibitive.

It's an ongoing challenge for MSPs and MSSPs to even keep up with a cyber security market in which technology trends evolve so quickly – let alone assess the relevance of those changes for their business models and service portfolios and adjust them rapidly. It's nevertheless one of the keys to an MSP or MSSP's success.

Integrating New Ideas into MSP and MSSP Business Models

Over the last couple of years, the rise of Secure Access Services Edge (SASE), the morphing of Endpoint Detection and Response (EDR) into the much broader Extended Detection and Response (XDR) and the rise of Zero Trust in the marketing of vendor portfolios has created challenges as well as opportunities. MSP and MSSP management has no choice but to spend a significant portion of its time assessing the relevance that these kinds of developments have to their target customers, and hence to the direction they set for their own business in serving them.

Only the very largest MSSPs that are making - or heading for - $1 billion a year in revenues can even consider being comprehensive managed security providers across all five of the NIST Cyber Security Framework's five pillars of Identify, Protect, Detect, Respond and Recover. Even many of those outsource parts of their portfolio to specialist partners. For a small MSP, trying to do too much, to be 'all things to all men' or 'a jack of all trades' in managed security, is one of the biggest mistakes they can make.

This White Paper looks at how MSPs and MSSPs should adapt their businesses to the accelerating momentum behind Zero Trust architectures, use cases and solutions. It examines the case for MSPs and MSSPs implementing Zero Trust themselves in their own environments and the case for them to sell Zero Trust solutions to customers. It also considers the case for tightly coupling their approach across those two domains.

Like it or not, the Term 'Zero Trust' is Here to Stay

Some vendors are failing to explain the need for supporting data classification and active software directory components to be in place.

Regrettably there is a lot of market confusion around what Zero Trust is. Much of it revolves around the term being used misleadingly in some vendor marketing. Too many vendors are slapping a 'Zero Trust' label on an existing product without offering much, if any, support for correlation with other contextual data or even occasional re-authorisation challenges. Too many vendors are speaking the 'silver bullet' language of Zero Trust transformation of an entire environment just by deploying one product in one part of the network. Some vendors are failing to explain the need for key enablers like basic data classification, active software directories and unified user directories spanning all business applications to be in place in order that the benefits they cite can even be derived from deploying their one product.

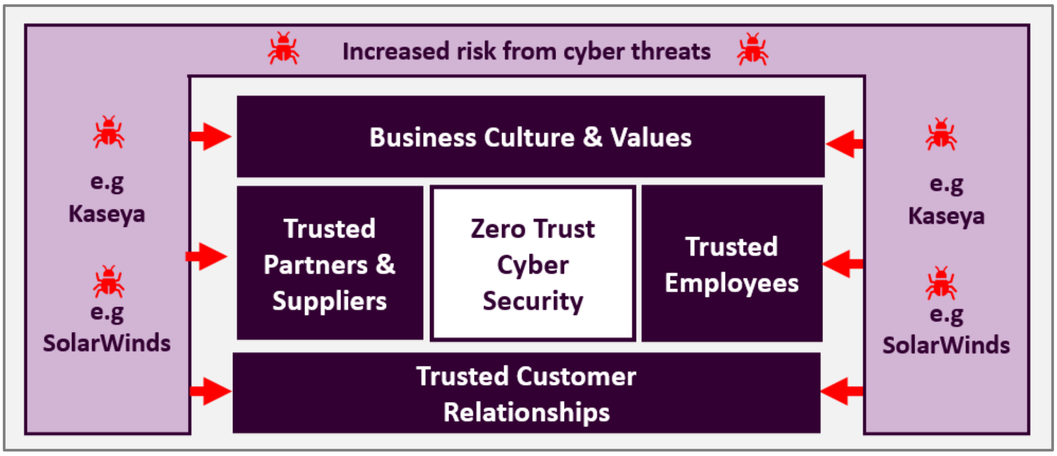
Purely from a cyber security perspective, 'Zero Trust' as a strategy or architecture, supported by a variety of products and product features, is the right way forward. We don't expect to check in at a major airport and from there be trusted to roam freely within the airport, go anywhere we like, board any aircraft we like, headed for any destination we like, any time we like. Instead, each individual accessing an airport – a passenger, a restaurant worker, a cleaner, a baggage controller, an air traffic controller, a flight attendant – is allocated their own unique set of access rights. Their identity and permissions are then continuously re-authenticated and re-verified as they go on to request access to different parts of the airport.

The Airport Security Analogy

The idea that this Zero Trust model of physical airport security is somehow not relevant to enterprise cyber security has, well, zero credibility. In cyber security we've made a lot of progress recognising that the centralized security perimeter is inevitably breached. Accordingly we've invested in detection and response to detect the threats that we now accept will inevitably get through. What we have barely started to address is the inherent trust that's embedded in the vast majority of software-based interactions between devices, networks, applications, and databases inside what's left of the perimeter.

It's this inherent trust which drives the blizzard of alerts in the SOC – and hence the fiendish complexity of today's co-called 'whac a mole' challenge in detection and response. Replacing interactions that are inherently trusted with ones that are instead subject to continuous checks and verifications in a way that is invisible to the user can substantially reduce risk. One of the ways it does that is by reducing the volume of alerts that make it through to the SOC – that gives the SOC greater certainty that the subset of alerts it sees in a less trusted environment are indeed worth investigating.

Figure 3: Zero Trust Security Needs Reconciling with Other Business Values


Increased risk from cyber threats
e.g Kaseya
e.g SolarWinds
Business Culture & Values
Trusted Partners & Suppliers
Zero Trust Cyber Security
Trusted Employees
Trusted Customer Relationships
e.g Kaseya
e.g SolarWinds

Source: HardenStance

Even though it is broadly speaking the right direction for cyber security, there are problems with the adoption of the term 'Zero Trust' within the user market. Marketeers – other than those working for cyber security vendors – tend to dislike it just because it sounds negative. C-Suite management can sometimes shy away from it too because they're uncomfortable using language that implies a distrust of employees in particular. The term can be especially challenging for MSPs and MSSPs – how can advocating Zero Trust make sense when your company's core mission is to persuade your customers that you can be their 'trusted partner'?

In September this year, the U.S. Office of Management and Budget (OMB) published draft guidance on Zero Trust implementation guidelines for federal agencies.

'Zero Trust' is Widely Used – "That Train Has Left the Station"

One can make the case that the term Zero Trust is imperfect and that an alternative term for describing the exact same principles might make it more appealing to non cyber security practitioners. But that's academic now. The term is now widely used throughout the cyber security industry. In September this year, the U.S. Office of Management and Budget (OMB) published draft guidance on Zero Trust implementation guidelines for federal agencies. In the UK, the National Cyber Security Centre (NCSC) recently did a similar thing, albeit in the form of recommendations rather than requirements. The Zero Trust ' train' has left the 'station', so to speak.

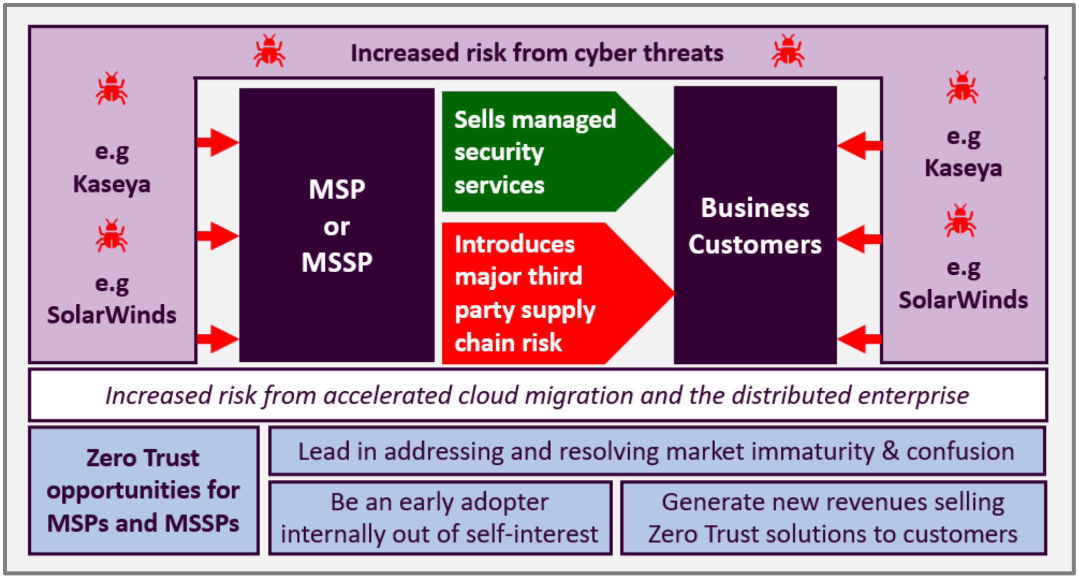
If MSPs and MSSPs want to be competitive, there is no realistic alternative to embracing Zero Trust, at least at some level. At minimum, MSPs need to be conversant in what it means and how it can be applied in a customer's unique environment. Preferably they need to be an active partner in enabling that transformation. There are some cases in business where not following the crowd is a smart move – Zero Trust isn't one of them.

The Right Language for Converting Sceptics

That still leaves the question of how to explain it. Some cyber security practitioners – some Zero Trust 'evangelists' in particular – have a tendency to speak to customers in terms of correcting their 'misunderstanding' or 'misinterpretation.' From a cyber security standpoint, they may well be right. But that doesn't mean that kind of language is the best approach to turning objectors or sceptics into converts.

It can convey a tone deaf indifference to the challenges customers face in filtering out what's true and what's not from the blizzard of conflicting Zero Trust marketing pitches they're being bombarded with. And it can convey a lack of empathy for the challenges customers face in trying to reconcile the way a cyber security term resonates with other aspects of their organization's values. Some of these may be far removed from cyber security but they are nevertheless at least as important to the success of the business.

Figure 4: Opportunity and Risk for MSPs and MSSPs in the Zero Trust Era


Increased risk from cyber threats
e.g Kaseya
e.g SolarWinds
MSP or MSSP
Sells managed security services
Introduces major third party supply chain risk
Business Customers
e.g Kaseya
e.g SolarWinds
Increased risk from accelerated cloud migration and the distributed enterprise
Zero Trust opportunities for MSPs and MSSPs
Lead in addressing and resolving market immaturity & confusion
Be an early adopter internally out of self-interest
Generate new revenues selling Zero Trust solutions to customers

Source: HardenStance

When considering what to do about Zero Trust, perhaps the biggest mistake an MSP or MSSP can make is to first ask how they can make money selling it.

One line of reasoning that can be effective is that it’s an employee’s digital identity whose authenticity and behaviour requires constant verification rather than the employee themselves. What can also help is to allude to other enterprise technology or products that have initially met with user resistance only to subsequently gain acceptance. One example is Security Incident Event Management (SIEM) platforms which encountered some objections to the way so many of an employee’s actions are automatically monitored and logged when they were first introduced.

Zero Trust is almost self-explanatory and self-evidently right for cyber security practitioners. Others can need more time. They need to have their objections listened to respectfully. They need to be persuaded that the benefits of Zero Trust outweigh their doubts. And they need to be convinced that the benefits can be delivered on time, within budget, and with a level of organizational change that is correctly scoped at the outset.

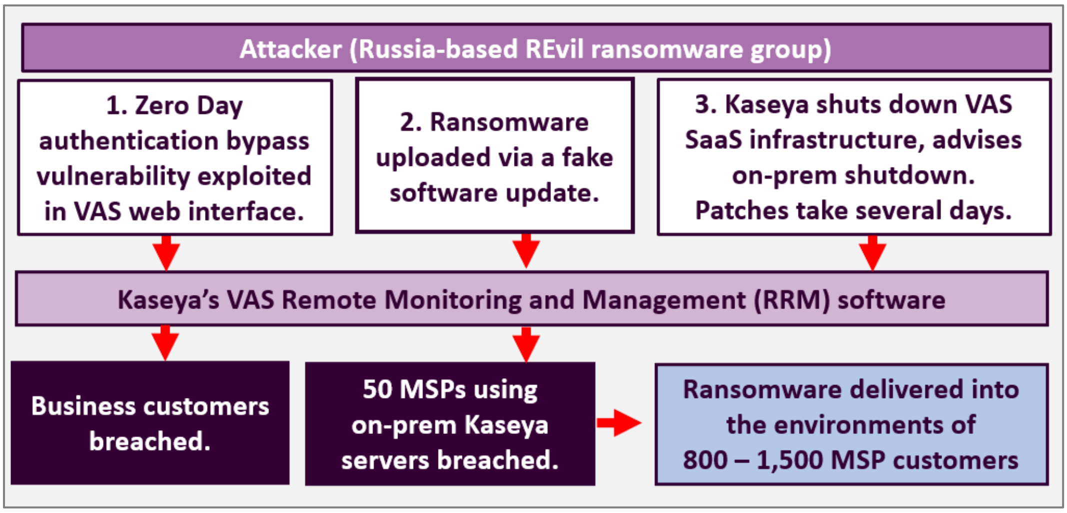
Zero Trust Begins at Home

When considering what to do about Zero Trust, perhaps the biggest mistake an MSP or MSSP can make is to first ask how they can make money selling it. Actually, the first question they should be asking is how they can adopt it in their own environment to protect their own business. Zero Trust should begin at home. This is because the anatomy of the SolarWinds and Kaseya breaches shows how many MSPs themselves served as lethal, albeit unwitting, enablers of those attacks. It also shows how embedded trust in the relationship between MSPs and their IT management software partners, as well as between MSPs and their customers, contributed to the terrible consequences.

As shown in **Figure 2** and **Figure 5**, both attacks left customer environments open to reconnaissance by threat actors. The SolarWinds attack then enabled privilege escalation leading to data exfiltration. That impacted several MSPs including SolarWinds MSP, the company’s own MSP business. The Kaseya breach exploited a zero day authentication vulnerability to deliver ransomware into the environments of between 800 – 1,500 customers via their MSP. The Kaseya breach also required the shutting down of the SaaS and on-prem variants of Kaseya’s Virtual System Administrator (VSA). That impacted availability and performance for all those MSPs’ customers for days.

Purely from a cyber security perspective there was – and for now at least, there still is – far too much embedded trust between these and other critical software providers and their MSP customers as well as between MSPs and their own customers. Clients attaching to these software vendors’ servers tend to perform whatever task is asked of them.

Figure 5: A Simplified Anatomy of the Kaseya Attack


Attacker (Russia-based REvil ransomware group)
1. Zero Day authentication bypass vulnerability exploited in VAS web interface.
2. Ransomware uploaded via a fake software update.
3. Kaseya shuts down VAS SaaS infrastructure, advises on-prem shutdown. Patches take several days.
Kaseya's VAS Remote Monitoring and Management (RRM) software
Business customers breached.
50 MSPs using on-prem Kaseya servers breached.
Ransomware delivered into the environments of 800 – 1,500 MSP customers

Source: HardenStance

Typically, hardly any verification is carried out on those instructions. This, together with the widespread use of this software by MSPs providing a gateway into hundreds or thousands of customers at one time, is exactly why these software vendors are such an attractive target for attackers. Introduction of greater – ultimately continuous - contextual verification of commands according to Zero Trust principles is critical to reducing the risk posed by attacks on these types of IT service provider.

It is clearly in the self-interest of MSPs and MSSPs to be early adopters of Zero Trust, entirely independently of whether they also want to sell Zero Trust services to customers.

Microsoft summarized the risk posed by the "Big Four" nation state cyber programs of Russia, China, Iran and North Korea in its October 2021 Digital Defense Report. Citing the Russia-based SolarWinds attack and the China-based attack on its own on-premises Exchange email systems, Microsoft stated that "the decision to target IT service providers in order to more successfully exploit victims downstream who receive services from those IT providers" represents "a revolutionary change." Although they have happened before – for example, UK MSPs were targeted with malware attacking a remote access tool by a China-based APT group in 2018 – it is not until very recently that they have been so devastatingly effective on such a large scale. Microsoft states this approach is now "common among all of the Big Four nation state cyber programs."

Better security features should certainly be built into their own software by SolarWinds, Kaseya, Microsoft and their peers. However, that can only be one part of the solution to reducing inherent trust in the relationship between these providers and their customers, be that an MSP or another user organization. Zero Trust principles mandate that the conditions on which some transactions are permitted can only be determined by the unique Zero Trust posture of a unique user organization itself.

It's in the Self-Interest of MSPs and MSSPs to be Early Adopters

What this points to is that it is clearly in the self-interest of MSPs and MSSPs to be early adopters of Zero Trust, entirely independently of whether they also want to sell Zero Trust services to customers. If they engage in an earnest risk assessment of their own business, then in most cases it's precisely the trusted interface between their own environment and their customers' environments that is an MSP's own 'crown jewels'. It's that interface that has been so dramatically shown to be a high risk vulnerability.

Embedding Zero Trust principles into an internal cyber security strategy to reduce the inherent risk in that interface should therefore be a critical business priority for any MSP or MSSP. Some large MSSPs already understand this. The entirety of their value proposition and their credibility revolves around cyber security.

However, that’s not the same for some MSPs, many of whom currently generate less than a third of their revenue from cyber security services. Many of these MSPs have been – some still are – remarkably complacent about their own internal cyber security posture. Traditionally, they’ve tried to do the bare minimum in security – and at the lowest possible cost. The continuing aftershock of the SolarWinds and Kaseya attacks should drive a fundamental reappraisal here, not least because some of the most security-conscious (therefore highest spending) customers are going to be asking more questions about the internal security of MSPs than in the past.

Finding the Right Niche in Zero Trust Services

Whatever label it ended up being given, Zero Trust was always going to come to the fore. It is front and centre now because of the answers it provides to some of the fundamental challenges in cyber security. The pandemic has caused a permanent shift in IT operations. Many businesses have gone from a small minority of employees working remotely to a large minority, and in some cases even a majority. This has ratcheted up the level of risk that organizations are exposed to. As shown, it isn’t just the overall risk from cyber threats that has risen in conjunction with the pandemic that makes Zero Trust relevant to MSPs and MSSPs - it’s the specific nature of some of that new risk.

Many MSPs have been – some still are – remarkably complacent about their own internal cyber security. They’ve tried to do the bare minimum in security – and at the lowest possible cost.

At this point in time, Zero Trust isn’t for everybody - or anything like everybody. Many organizations are way behind on basic cyber security hygiene like Two Factor Authentication and logging detection (or even best practise password rotation). The proportion will certainly increase over time but today, only a minority of businesses are ripe for even reviewing their cyber security posture and strategy from a Zero Trust perspective. It’s then a next step to initiate a first small scale project, and then build on the learnings from that to replace trusted relationships with continuous verification elsewhere in the organization.

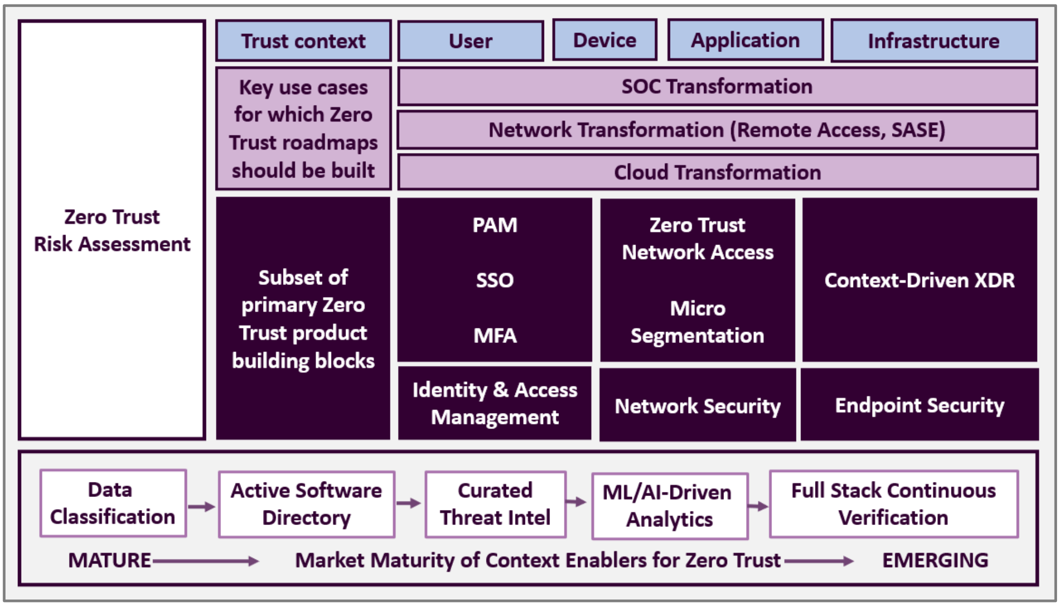
‘Horses for Courses’

The outlook of MSPs and MSSPs considering whether to sell Zero Trust products and services is as diverse as it is for customer organizations considering buying them. Some Managed Detection and Response (MDR) providers that are determined to focus on just that space tend to be most interested in improving the efficacy of their SOC operations. They can do this by integrating with Zero Trust-enabling Identity and Access Management and network security controls deployed and managed by someone else. At another extreme, a lot of MSPs generating less than 20% of their revenue from security see no sense in committing to Zero Trust services at this early stage of the market.

It’s the players who occupy the middle ground that should be highly motivated to view Zero Trust as an emerging revenue opportunity. This includes fully-fledged MSSPs who are positioned as across-the-board providers of managed security services. They can look at the Zero Trust services opportunity as represented in **Figure 6** and either extend existing competences or build new ones to target almost any of the markets, products or solution use cases depicted. This fertile middle ground also includes MSPs who currently have a limited cyber security capability but want to grow it; those who are already strong in cyber security and plan on staying that way; and those who are already strong but want to drive deeper into the security market to become a focused MSSP. These latter types of MSP need to be very discerning in where they choose to play.

Wholly independent of the mindshare Zero Trust has started taking in the cyber security market, large buyers and large sellers like big vendors, MSPs and MSSPs consistently report the same trends in cyber security purchasing. Driven by the greater complexity arising from software-driven dependencies as well as a drive to improve security efficacy and cost efficiency, the core trend in cyber security purchasing in recent years is away from simple product resale and towards sales that are more integrated at an architectural or use case level, hence they require multiple integrated or pre-integrated

Figure 6: Finding the Right Niche in Zero Trust Services


Zero Trust Risk Assessment
Trust context
User
Device
Application
Infrastructure
Key use cases for which Zero Trust roadmaps should be built
SOC Transformation
Network Transformation (Remote Access, SASE)
Cloud Transformation
Subset of primary Zero Trust product building blocks
PAM
SSO
MFA
Zero Trust Network Access
Micro Segmentation
Context-Driven XDR
Identity & Access Management
Network Security
Endpoint Security
Data Classification
Active Software Directory
Curated Threat Intel
ML/AI-Driven Analytics
Full Stack Continuous Verification
MATURE
Market Maturity of Context Enablers for Zero Trust
EMERGING

Source: HardenStance

products or software components. One example is the market's evolution in recent years from standalone SD-WAN and network security products to secure SD-WAN solutions and now Secure Access Services Edge (SASE) with Zero Trust capabilities baked in.

Most organizations don't have a proper understanding yet of what's even required to drive out embedded trust in terms of people, processes and technology.

As suggested in **Figure 6,** the nascent market in Zero Trust products and services is evolving in a direction that aligns closely with these trends, and even accelerates them. Some small amount of inherent trust can certainly be reduced by dropping in a single product supporting better verification features into an existing environment. That's fine as far as it goes. However replicating that model over and over again, individual security control by individual security control, doesn't scale well. Just as importantly, it's missing a coherent, unified Zero Trust target architecture to aim for.

A 'Grand Masterplan' is almost certainly Doomed to Fail

The opposite extreme – some grand organization-wide masterplan beginning at the end of the year and due to be completed within three years – is highly unlikely to work either. Most organizations don't have a granular understanding yet of what's even required to drive out embedded trust in terms of the different dimensions of people, processes and technology. In large organizations in particular, a top-down grand masterplan is almost certainly doomed to fail.

Figure 6 depicts three of the most popular IT transformation and cyber security use cases that organizations will continue investing heavily in over the next few years. As shown, these are Network Transformation (including remote access and SASE); Cloud Transformation and SOC Transformation. Anyone looking to deploy any of these use cases nowadays should be looking to embed support for Zero Trust features of continuous verification, authentication and authorisation.

Naturally, not all the capabilities are available for enabling Zero Trust to be implemented fully-featured, end to end, across a customer organization. We are some way off being able to perform continuous verification every few minutes, let alone every few seconds, throughout the security stack according to a desired Zero Trust end state. Nevertheless, many widely available products already support valuable subsets of those features, and these will be added to over time.

The three examples cited above are by no means the only market niches that an MSP or MSSP can look to prioritize in building out a portfolio of Zero Trust services. They nevertheless demonstrate that while it is a set of all-embracing principles applicable throughout an end to end security architecture, Zero Trust can nevertheless be broken down into discrete, manageable components. Any MSP or MSSP should be able to identify one or more Zero Trust niches to specialize in, enabling them to enter this market in a focused way that assures a good return on investment.

Assembling the Right Coalition of Partners

MSPs and MSSPs should fully exploit the increasingly software-driven dynamism and diversity of the market in IT and cybersecurity products and services. This is a market that seems set to continue proliferating and diversifying via new start-ups and current players entering new market spaces - even while it also continues consolidating via mergers and acquisitions among MSPs, MSSPs, IT vendors and cyber security vendors.

There are so many market spaces an MSP or MSSP can participate in according to a variety of hybrid self-build/outsource and simple resale/managed models. You can do your own infrastructure penetration testing but partner someone else for web application pen testing. You can build a SOC and staff it from 9.00 – 5.00 but then outsource out-of-hours SOC management to a SOC as a Service partner. You can host leading vendor solutions yourself or integrate and resell them as a SaaS offering. As an MSP you can choose not to partner a much larger MSSP in any way, or alternatively serve as a channel for one or several of their services.

Just as many Zero Trust solutions are made up of multiple components, so an MSP and MSSP's approach to building a Zero Trust services portfolio should exploit the rich diversity of different partners as well as the variety of go-to-market models that many of them are able to support. There are many more winning business models for MSPs and MSSPs to find from mixing and matching from among available partners than there are from assuming they have to staff up and do most of this themselves.

Clearly, a tight coupling between internal and market portfolio strategies can deliver significant business benefits.

Aligning Internal and Market Portfolio Strategies

This White Paper has made separate, stand-alone, cases for MSPs and MSSPs to invest in Zero Trust internally as well as invest in a Zero Trust services portfolio to sell to customers. That leaves open the question of how tightly coupled these two should ideally be. Can you be credible selling Zero Trust services if you have no experience of deploying it yourself in your own environment – if you aren't 'eating your own dog food' ? Equally, does it make no sense to invest internally but then decline the opportunity to sell any Zero Trust services at all?

There are several nuanced layers to this rather than any clean and simple answers. First, being a successful early adopter of Zero Trust will enhance any MSP or MSSP's credibility as a trusted partner. Projecting your efforts to protect your own organization via an internal Zero Trust deployment in the wake of the Kaseya and SolarWinds attacks will be generally well received by customers - because, by implication, that investment protects them too. That credibility boost is independent of whether all, some, or none of your business even comes from managed security. Moreover, if you do offer managed security services, your entire security portfolio should benefit by association – whether it includes any Zero Trust propositions or not.

Clearly, a tight coupling between internal and market portfolio strategies can deliver significant business benefits. Take an example of an MSP or MSSP that undertakes a remote access network transformation within its own environment. It upgrades Identity and Access Management (IAM) controls with Privileged Access Management (PAM) and introduces Zero Trust Network Access (ZTNA) and micro-segmentation.

The MSP or MSSP that gets ahead of the curve deploying that internally should be well placed to assemble a compelling Zero Trust Network Transformation solution offer to customers. The solution can have the credibility of being built around the MSP or MSSP's own experience in the real world. Critically it can be both repeatable and differentiated.

There may not be as much value in loosely coupled or wholly decoupled approaches but that's not a reason to avoid them. An MSP or MSSP's own internal priority may be to deploy Zero Trust in a Network Transformation use case. But if it's background is in SOC-based detection and response – or it can assemble the right partners to be successful with SOC Transformation use cases that embed Zero Trust capabilities - there is no reason for that company not to move forward with a strategy where the internal and customer-facing priorities are different. ■

About the Sponsors

The sponsors of this White Paper are CyberArk and Palo Alto Networks.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit https://www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk LinkedIn or Facebook.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, MEF, OASIS, The GSM Association, ETSI and The Cyber Threat Alliance. HardenStance is also a recognised Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com