Beyond Security, Zero Trust for Business Enablement

Heng Mok – CISO APJ

Agenda

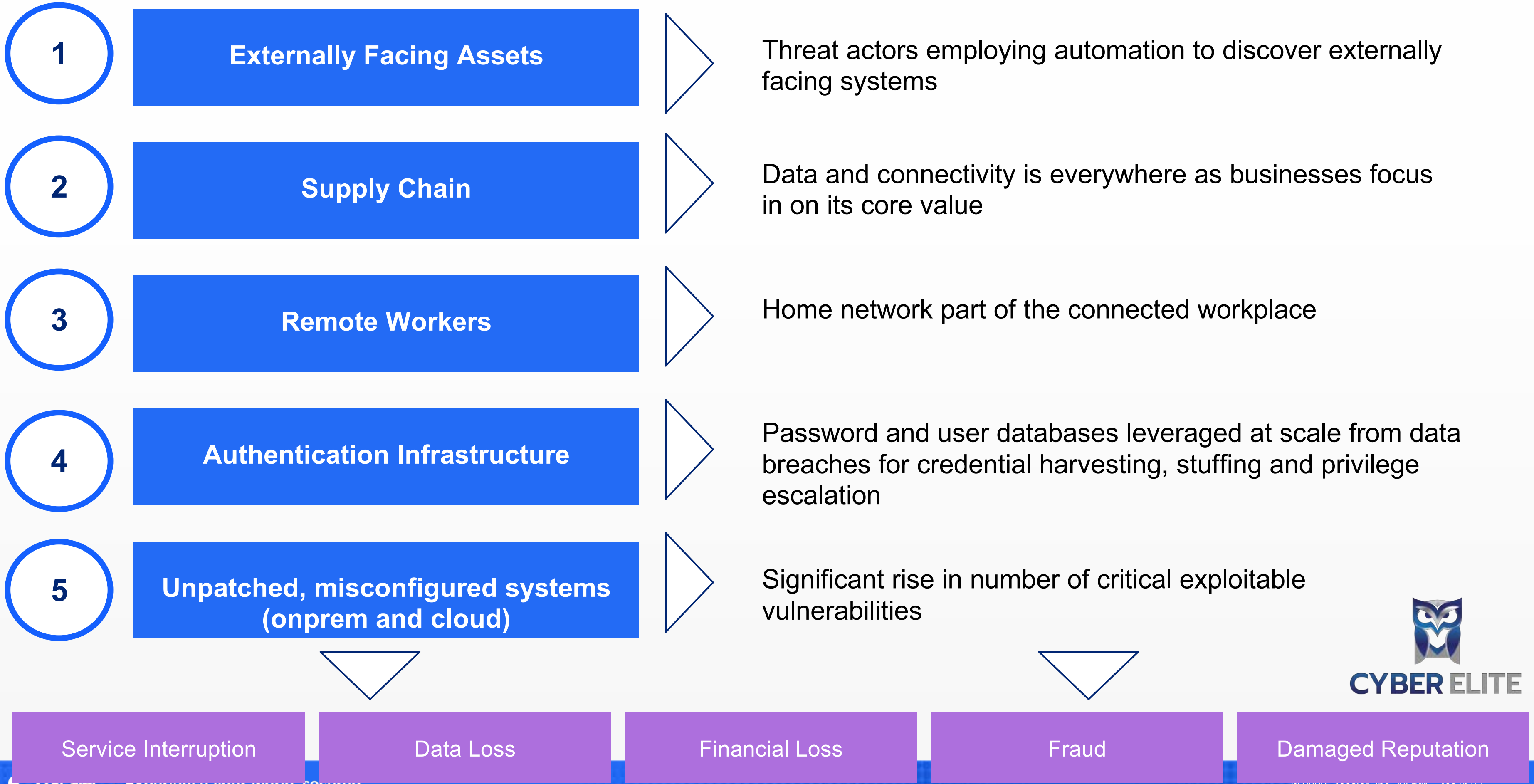
- Business and Security Context
- Zero Trust Simplified
- Real World Use Cases
- Zero Trust Architecture in Cost Avoidance
- Where do I start in my Zero Trust Journey
- Summary
- Resources

CYBER ELITE

Business and Security Context

CYBER ELITE

Threat Landscape



1. **Externally Facing Assets** – Threat actors employing automation to discover externally facing systems

2. **Supply Chain** – Data and connectivity is everywhere as businesses focus in on its core value

3. **Remote Workers** – Home network part of the connected workplace

4. **Authentication Infrastructure** – Password and user databases leveraged at scale from data breaches for credential harvesting, stuffing and privilege escalation

5. **Unpatched, misconfigured systems (onprem and cloud)** – Significant rise in number of critical exploitable vulnerabilities

Service Interruption | Data Loss | Financial Loss | Fraud | Damaged Reputation

Reducing Cost & Complexity Is a Priority in Today's Economy

The workplace is changing

- Users are working everywhere
- Apps and data are widely distributed

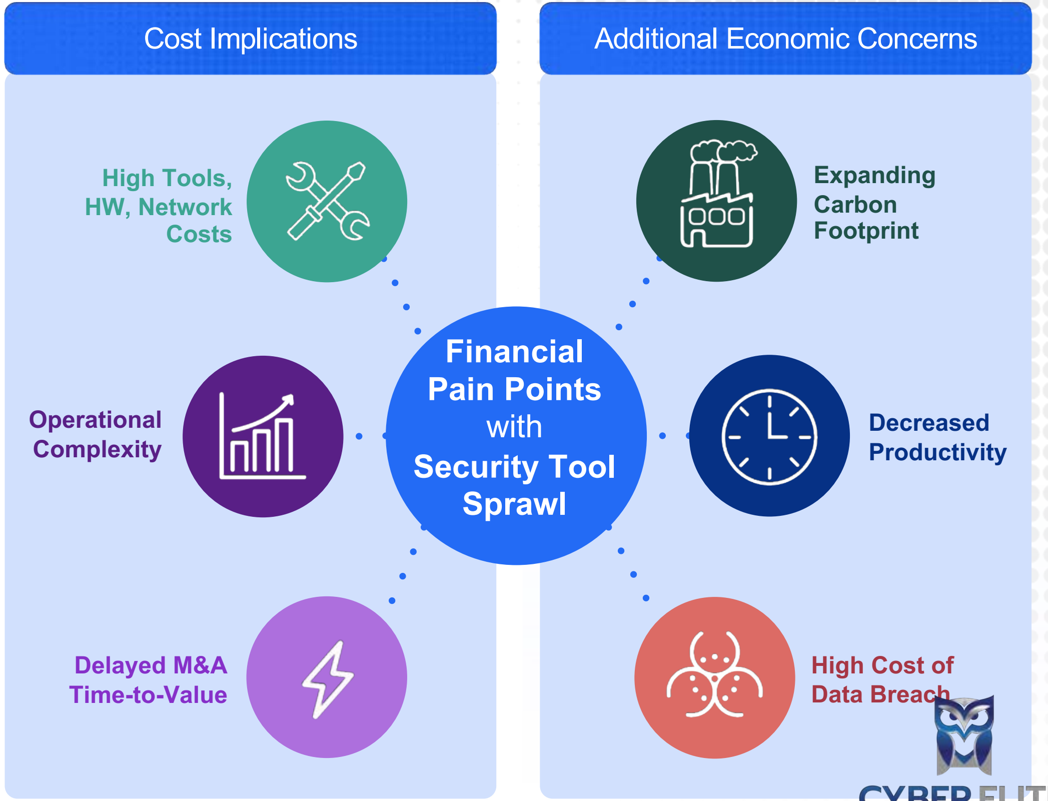
New challenges are on the rise

- Economic uncertainty
- Sophisticated cyberthreats

Time-tested approaches fall short

- Traditional networks and perimeter security expose distributed organizations to increased risk and costs

75% of enterprises pursuing security vendor consolidation
(up from 29% previous year)
Gartner, "Top Trends in Cybersecurity" 2022


Cost Implications
Additional Economic Concerns
High Tools, HW, Network Costs
Operational Complexity
Delayed M&A Time-to-Value
Financial Pain Points with Security Tool Sprawl
Expanding Carbon Footprint
Decreased Productivity
High Cost of Data Breach

CYBER ELITE

What is Zero Trust

In simple terms.

CYBER ELITE

What is Zero Trust?

Zero Trust is:

…Much more than just Technology. It is a framework for securing organizations in the cloud and mobile world that asserts that no user or application should be trusted by default

…Transformative Re-imagining how you manage cybersecurity to better align to the way you do business

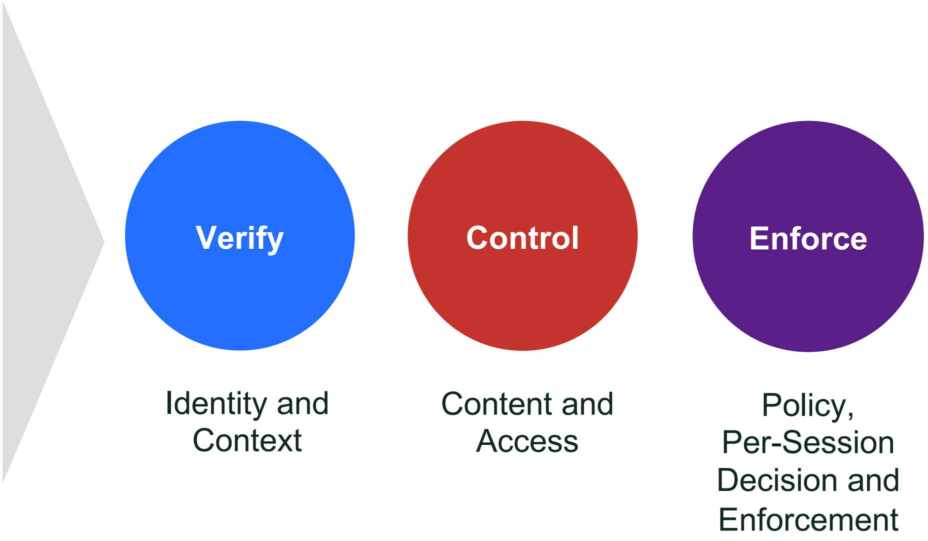
Zero Trust is not:

…An out of the box technology solution

…Multifactor Authentication

…least Privilege Identity and Access management

…adding more Firewalls



Verify

Identity and Context

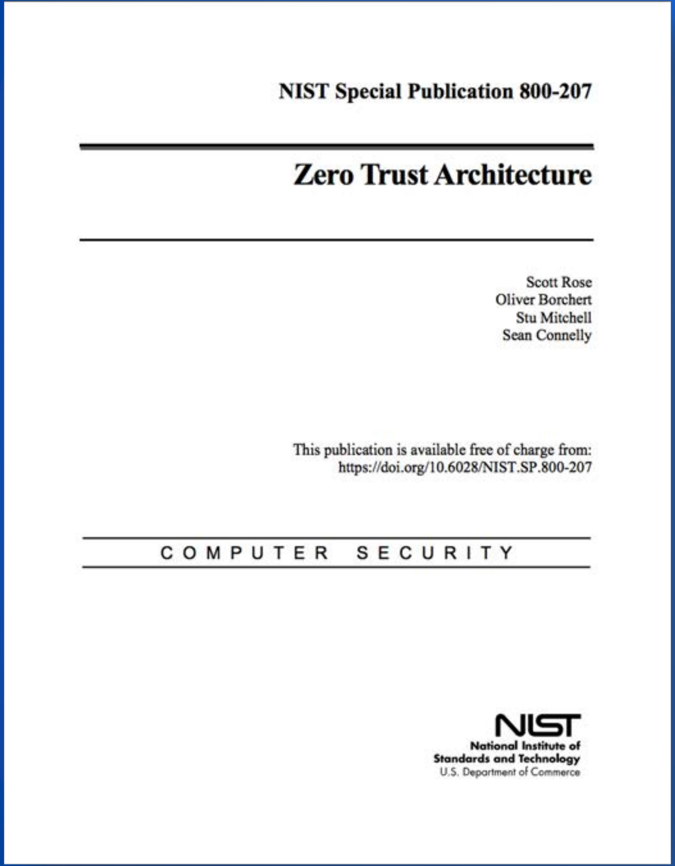
Control

Content and Access

Enforce

Policy, Per-Session Decision and Enforcement

CYBER ELITE



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

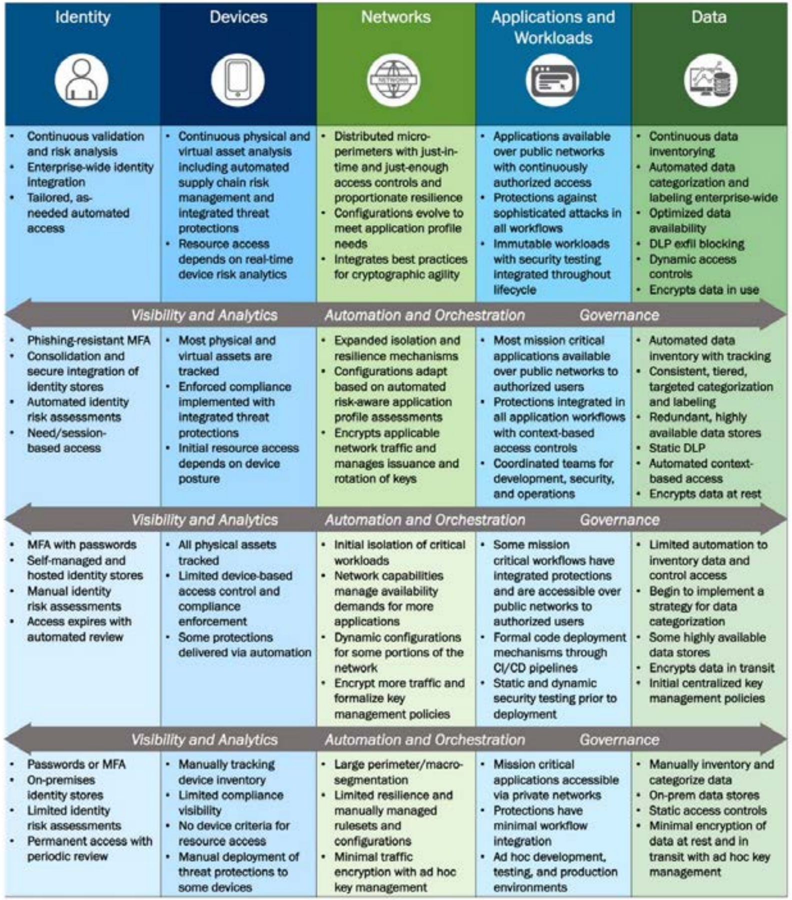
> “Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.”

- NIST Special Publication 800-207

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

CYBER ELITE

Zero Trust Maturity Model (CISA)



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
		Visibility and Analytics		Automation and Orchestration	Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
		Visibility and Analytics		Automation and Orchestration	Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
		Visibility and Analytics		Automation and Orchestration	Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

- Adopting Zero Trust is not a one-size-fit-all approach and every organization’s journey may be different considering its business priorities, complexity, technology landscape and regulatory requirements
- CISA Maturity Model V2 released in April 23

CYBER ELITE

Real World Use Cases for Business Enablement

Work from Anywhere

CYBER ELITE

Context – Work from Anywhere

“In a post COVID world remote working has become the norm”

“New employment markets are opened”

“Over the last 2 years new habits have been shaped by employees working flexibly and remotely”

“Offering flexible, secure remote working is an intangible business benefit for staff retention”

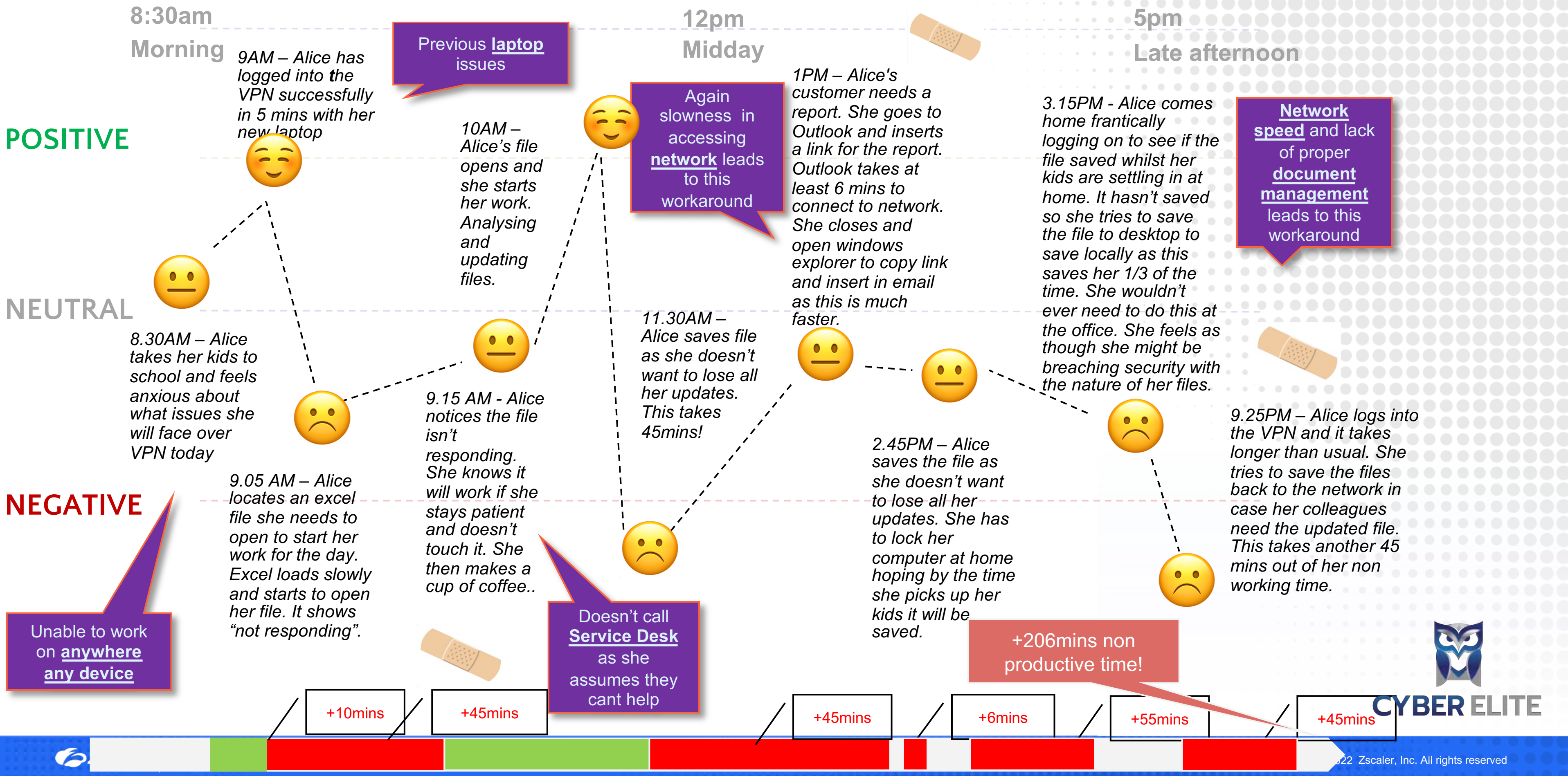
“Productivity has not decreased as a result of remote working”

“Cultural barriers have been broken in certain countries where previous expectations are no longer physically possible”

“Employee experience is becoming as important as the customer experience”

CYBER ELITE

The VPN Experience



8.30AM – Alice takes her kids to school and feels anxious about what issues she will face over VPN today

9AM – Alice has logged into tthe VPN successfully in 5 mins with her new laptop

Previous **laptop** issues

9.05 AM – Alice locates an excel file she needs to open to start her work for the day. Excel loads slowly and starts to open her file. It shows "not responding".

Unable to work on **anywhere any device**

9.15 AM - Alice notices the file isn't responding. She knows it will work if she stays patient and doesn't touch it. She then makes a cup of coffee..

10AM – Alice's file opens and she starts her work. Analysing and updating files.

Doesn't call **Service Desk** as she assumes they cant help

Again slowness in accessing **network** leads to this workaround

11.30AM – Alice saves file as she doesn't want to lose all her updates. This takes 45mins!

1PM – Alice's customer needs a report. She goes to Outlook and inserts a link for the report. Outlook takes at least 6 mins to connect to network. She closes and open windows explorer to copy link and insert in email as this is much faster.

2.45PM – Alice saves the file as she doesn't want to lose all her updates. She has to lock her computer at home hoping by the time she picks up her kids it will be saved.

3.15PM - Alice comes home frantically logging on to see if the file saved whilst her kids are settling in at home. It hasn't saved so she tries to save the file to desktop to save locally as this saves her 1/3 of the time. She wouldn't ever need to do this at the office. She feels as though she might be breaching security with the nature of her files.

Network speed and lack of proper **document management** leads to this workaround

9.25PM – Alice logs into the VPN and it takes longer than usual. She tries to save the files back to the network in case her colleagues need the updated file. This takes another 45 mins out of her non working time.

+206mins non productive time!

+10mins

+45mins

+45mins

+6mins

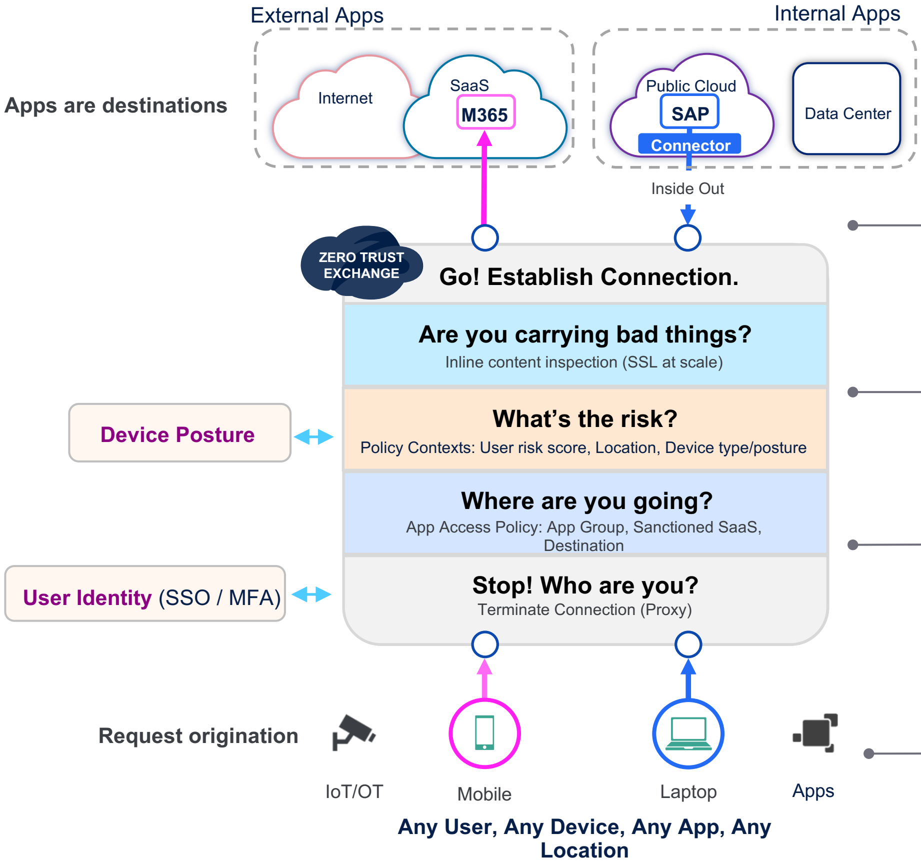
+55mins

+45mins

CYBER ELITE

Zero Trust Architecture for Work from Anywhere

Fast, performant and resilient access



Apps are destinations

External Apps

Internet

SaaS

M365

Internal Apps

Public Cloud

SAP

Connector

Data Center

Inside Out

ZERO TRUST EXCHANGE

Go! Establish Connection.

Are you carrying bad things?
Inline content inspection (SSL at scale)

What's the risk?
Policy Contexts: User risk score, Location, Device type/posture

Where are you going?
App Access Policy: App Group, Sanctioned SaaS, Destination

Stop! Who are you?
Terminate Connection (Proxy)

Device Posture

User Identity (SSO / MFA)

Request origination

IoT/OT

Mobile

Laptop

Apps

Any User, Any Device, Any App, Any Location

Peering and fast access to cloud services

Reducing the performance burden and backhauling by going direct to applications

Smart, redundant routing to the application

Bring the security edge closer to the user and cloak externally facing applications

Any device, any-where at anytime with a modern seamless experience

Use Cases

Permanent Hybrid Work

Secure High Risk Connectivity

Policy Driven Least Privileged Access

CYBER ELITE

Real World Use Cases for Zero Trust

Supporting Transformation

CYBER ELITE

Zero Trust Supporting Business Transformation

Business / Technology Transformation Agenda	Use Case	Description
Customer Transformation	DevOps and ways of working	Automation which improves speed and velocity Digital networks Open / Guest internet services
Employee Transformation	Securing mobile worker devices	Secure remote access for rugged devices for business processes such as asset management, mobile banking and sales
	Secure and provide fast access to SaaS	Secure SaaS applications - HR, Logistics and collaboration
Cloud	Secure outbound communication	Proxy based protection for workloads communicating with 3rd party APIs Secure non connected non production environments
Infrastructure Simplification	Improved resilience	DR and business continuity remote access improvements (multi region / DC routing) Firewall consolidation Cost optimisation through MPLS decomm to SD WAN Policy driven management Improved user experience and performance (o365 and connector to application routing) Café like experience for back office workers
M and A	Business agility	Project extension into shared or temporary office space Day 1 integration scenarios

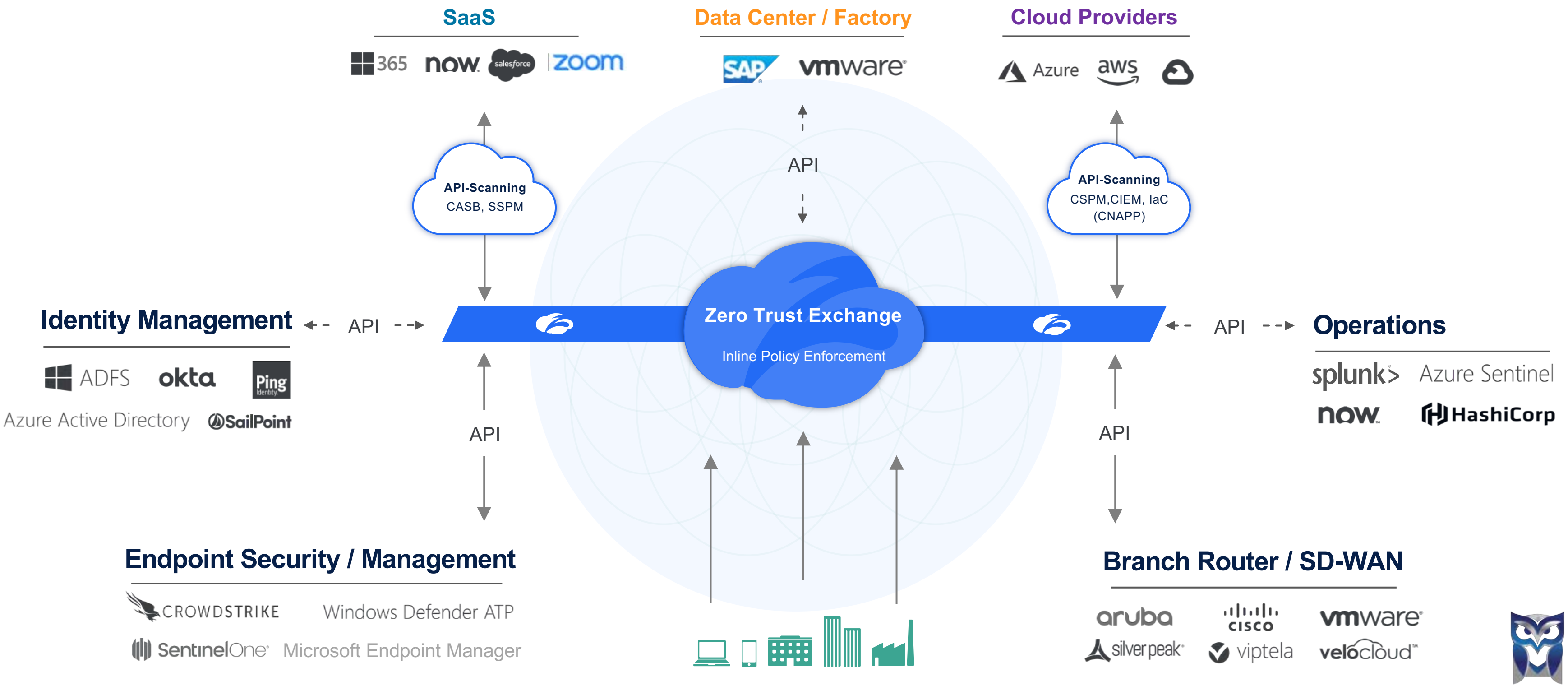
CYBER ELITE

Business case for cost optimisation

Zero Trust

CYBER ELITE

Platforms eliminate point solutions & allow for vendor consolidation



SaaS

365 now salesforce zoom

API-Scanning
CASB, SSPM

Data Center / Factory

SAP vmware

API

Cloud Providers

Azure aws

API-Scanning
CSPM,CIEM, IaC
(CNAPP)

Identity Management

API

ADFS okta Ping Identity
Azure Active Directory SailPoint

Zero Trust Exchange

Inline Policy Enforcement

API

Operations

splunk> Azure Sentinel
now HashiCorp

API

API

Endpoint Security / Management

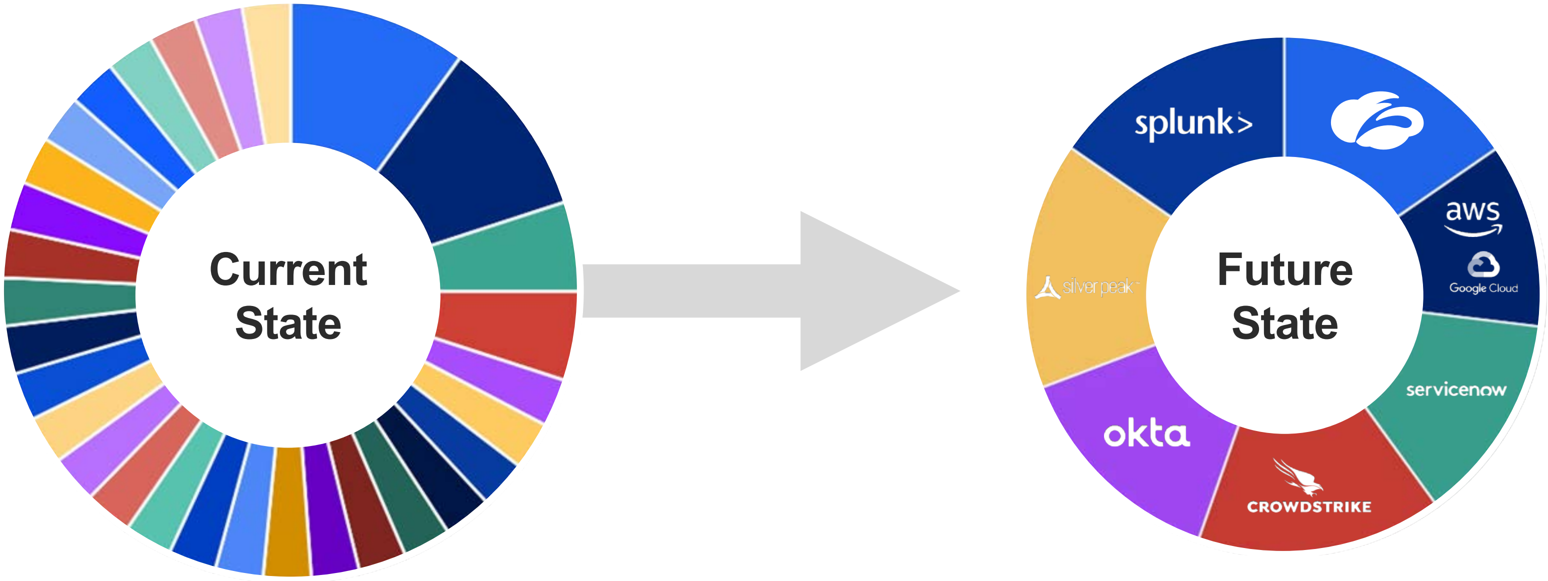
CROWDSTRIKE Windows Defender ATP
SentinelOne Microsoft Endpoint Manager

Branch Router / SD-WAN

aruba cisco vmware
silver peak viptela velocloud

CYBER ELITE

Replace, Reduce, Avoid



Current State

Future State

At least 30[1] disparate point solution, hardware & appliance vendors requiring complex integration and manual operational management

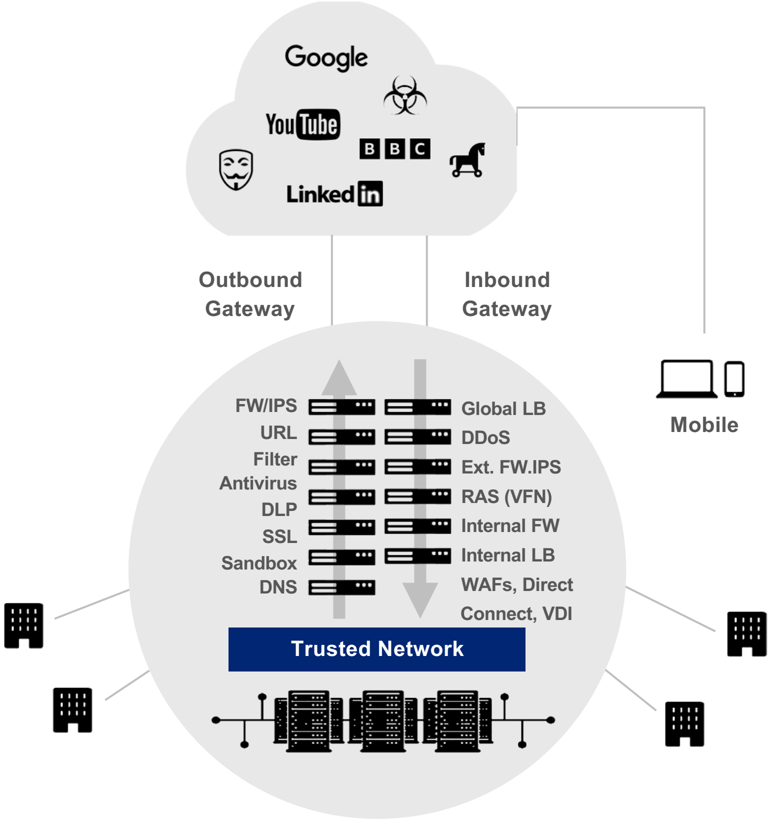
Best-in-class integrated solutions with ease of management[2]

[1] IBM Cyber Resilient Organization Study 2021

[2] Sample reference architecture

* Third-party logos remain the property of their respective owners and are not meant to convey a relationship or endorsement.

Do More With Less: Cost of Managing Multiple Vendors



Duplicative Costs

Licensing
Subscription
FTE Support (!)

Hidden Costs

Increased training
Lack of integration
Services/Maintenance compatibility issues
Excess vendor management time
Heavy burden from Procurement, Commercial, and Operational teams
Lack of personal relationship w/ vendor
Multiple payments to one provider
Complex SLA management and supplier performance monitoring
Poor unit pricing/negotiation leverage

CYBER ELITE

Zero Trust Architecture – Delivers a strong ROI

	Internet Access	Private App Access	Networking	Secure Cloud Data
Cost Savings **DMZ** 3-6 Hubs/DCs	**Outbound DMZ** Firewall / IPS Proxy/URL filter Anti-virus DLP SSL inspection Sandbox	**Inbound VPN** Load balancing VPN concentrators DDoS VDI / Citrix	**MPLS** (SD-WAN) **Microsegmentation** **Network & Endpoint Monitoring Tools**	
Cloud Gateway Multi-Cloud, Multi-Regions	**Virtual DMZ** Cloud Firewalls Cloud Proxies	**Virtual VPN** Load Balancing VPN Concentrators	**Site-to-Site VPN** Cloud-to-Cloud Cloud-to-DC	**Security Point Products** CASB, SSPM CSPM, CIEM, IaC
Operational Savings	Point product management / integration Policy management Automation (M365, API integrations)	Point product management / integration App access policy management	Routing complexity Network micro-segmentation Performance troubleshooting	Point product management / integration Risk Prioritization

Risk Reduction

Business Disruption
A cyber breach can impact operations, Maersk, Colonial Pipeline
What's the cost of business disruption per hour?

Data Protection
Avoid Liability: Loss of customer data, PHI
Maintain Competitiveness: Loss of IP

Brand reputation
Potential loss of future business (Equifax, Target)

Agility & Productivity

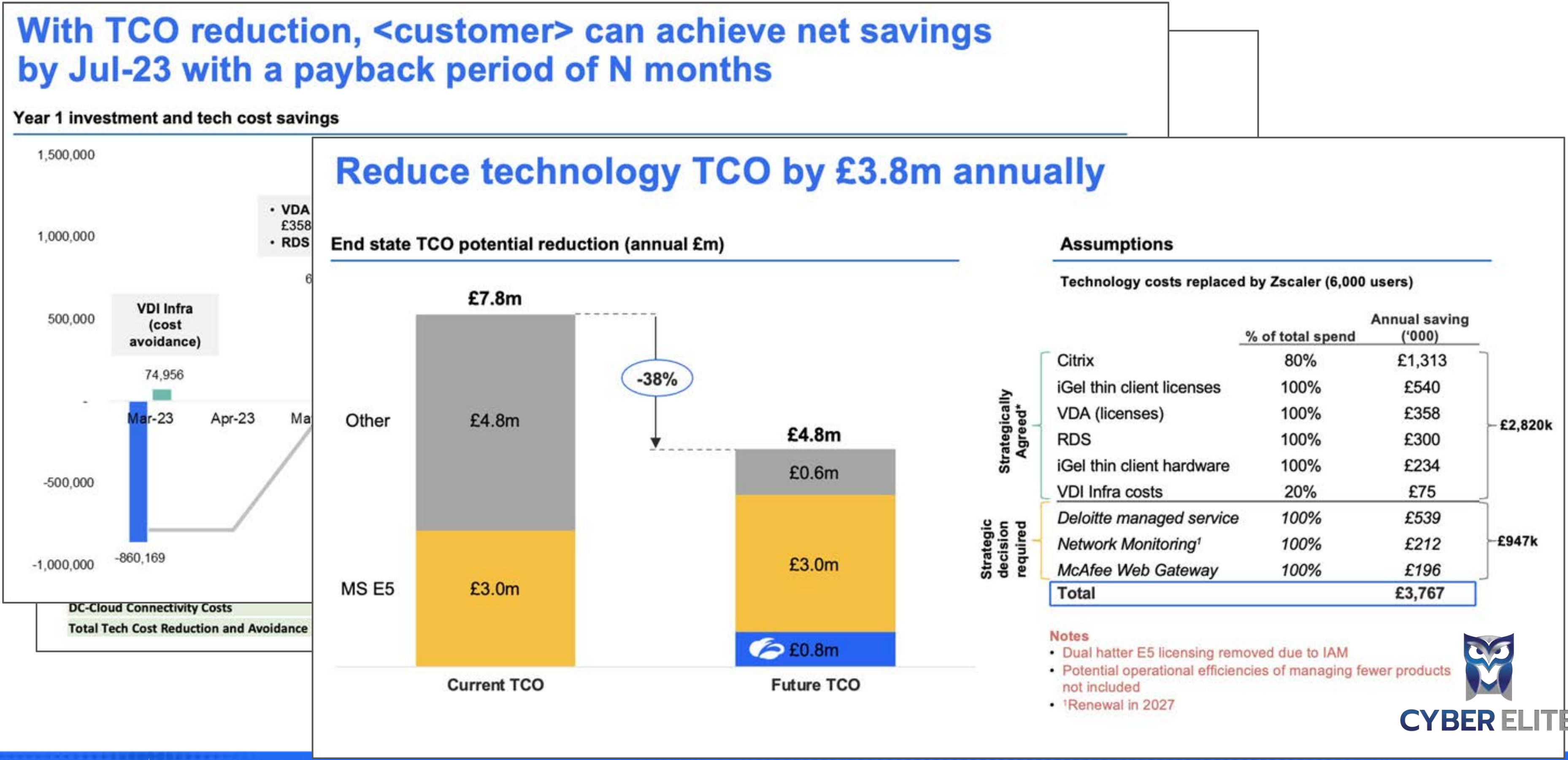
App Performance: Peering, Prioritization

User Experience: Reduced latency, Faster issue resolution

3rd Party Access, M&A, Divestitures: IT integration without integrating the network

CYBER ELITE

(1) Cost Savings



With TCO reduction, <customer> can achieve net savings by Jul-23 with a payback period of N months

Year 1 investment and tech cost savings

1,500,000
1,000,000
500,000
-
-500,000
-1,000,000
VDI Infra (cost avoidance)
74,956
-860,169
Mar-23
Apr-23
Ma
• VDA £358
• RDS
6
DC-Cloud Connectivity Costs
Total Tech Cost Reduction and Avoidance

Reduce technology TCO by £3.8m annually

End state TCO potential reduction (annual £m)

Assumptions

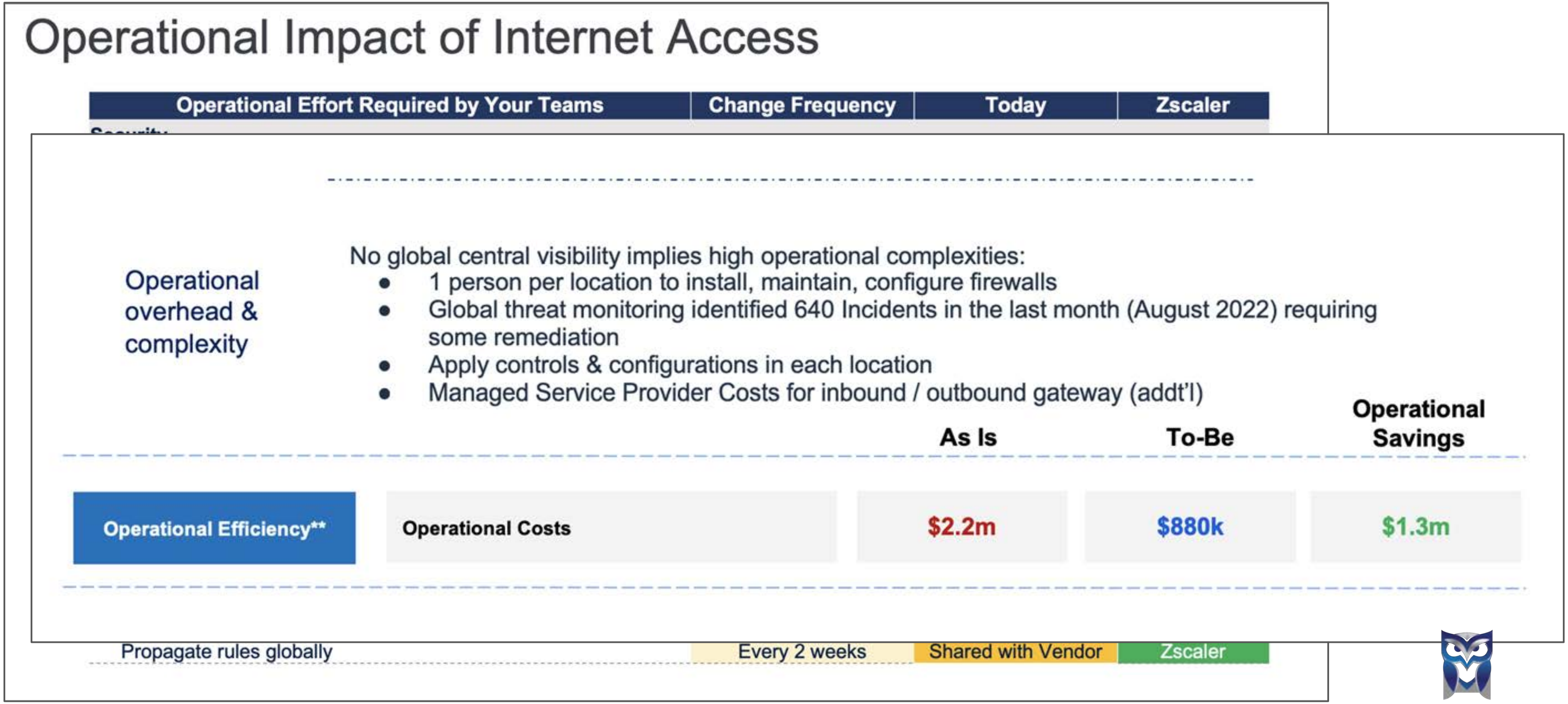
Technology costs replaced by Zscaler (6,000 users)

		% of total spend	Annual saving ('000)	
Strategically Agreed*	Citrix	80%	£1,313	£2,820k
	iGel thin client licenses	100%	£540	
	VDA (licenses)	100%	£358	
	RDS	100%	£300	
	iGel thin client hardware	100%	£234	
	VDI Infra costs	20%	£75	
Strategic decision required	*Deloitte managed service*	*100%*	*£539*	£947k
	Network Monitoring[1]	*100%*	*£212*	
	McAfee Web Gateway	*100%*	*£196*	
	Total		£3,767	

Notes

- Dual hatter E5 licensing removed due to IAM
- Potential operational efficiencies of managing fewer products not included
- [1]Renewal in 2027

(2) Operational Savings



Operational Impact of Internet Access

Operational Effort Required by Your Teams	Change Frequency	Today	Zscaler
Propagate rules globally	Every 2 weeks	Shared with Vendor	Zscaler

Operational overhead & complexity

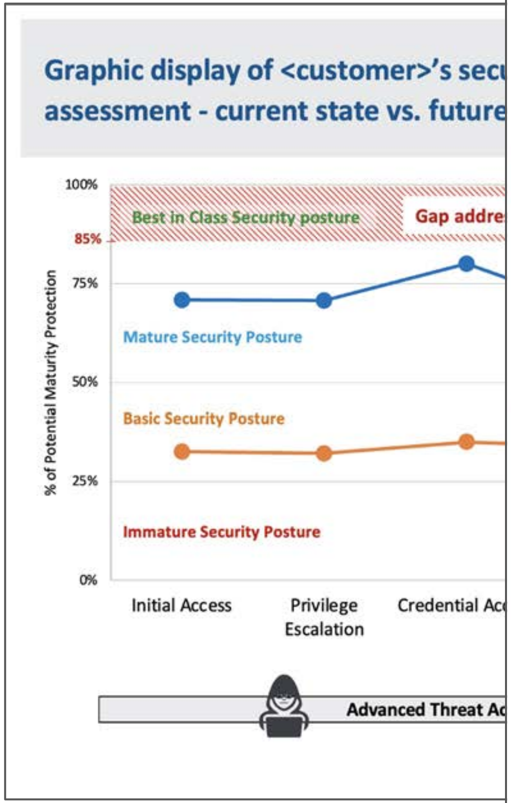
No global central visibility implies high operational complexities:

- 1 person per location to install, maintain, configure firewalls
- Global threat monitoring identified 640 Incidents in the last month (August 2022) requiring some remediation
- Apply controls & configurations in each location
- Managed Service Provider Costs for inbound / outbound gateway (addt'l)

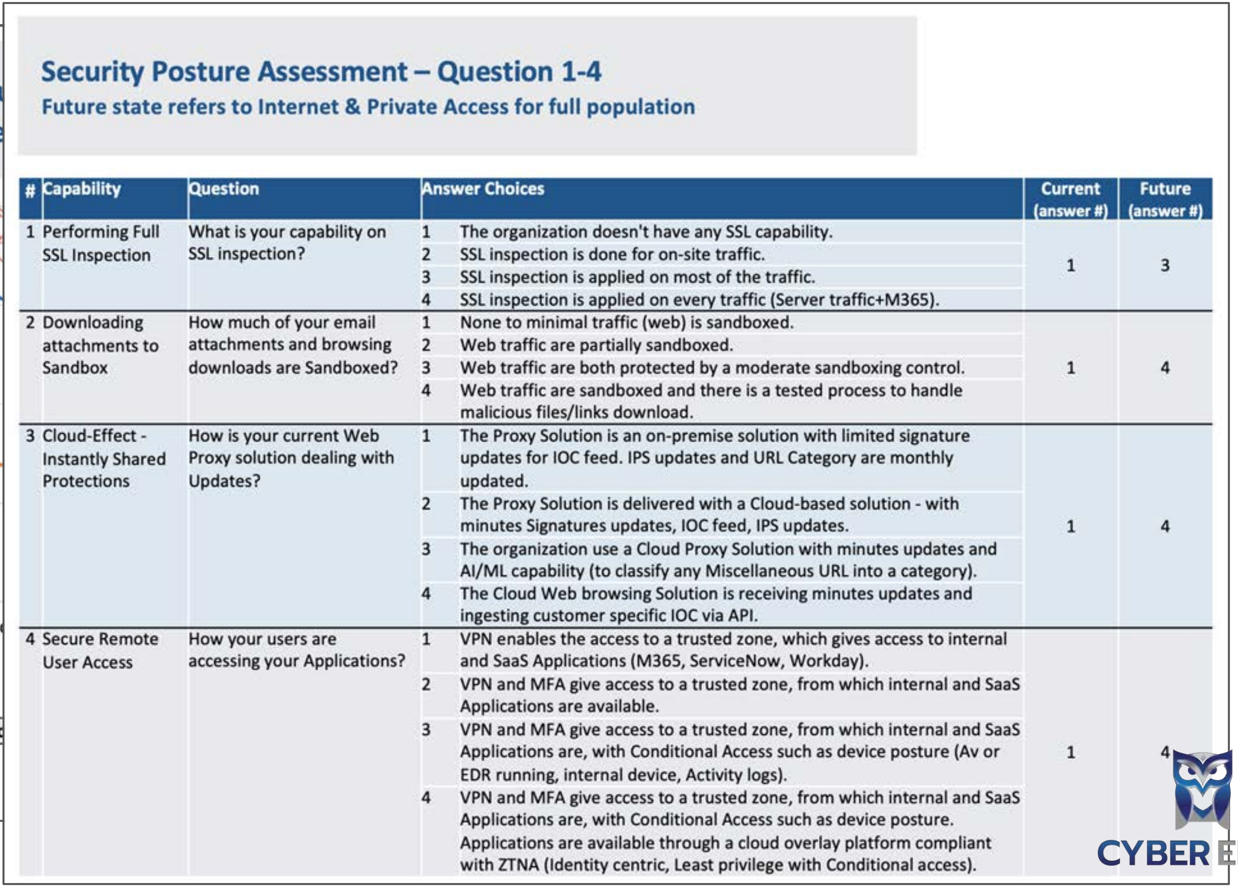
		As Is	To-Be	Operational Savings
Operational Efficiency**	Operational Costs	$2.2m	$880k	$1.3m

CYBER ELITE

(3) Risk Reduction



Graphic display of <customer>'s secu
assessment - current state vs. future



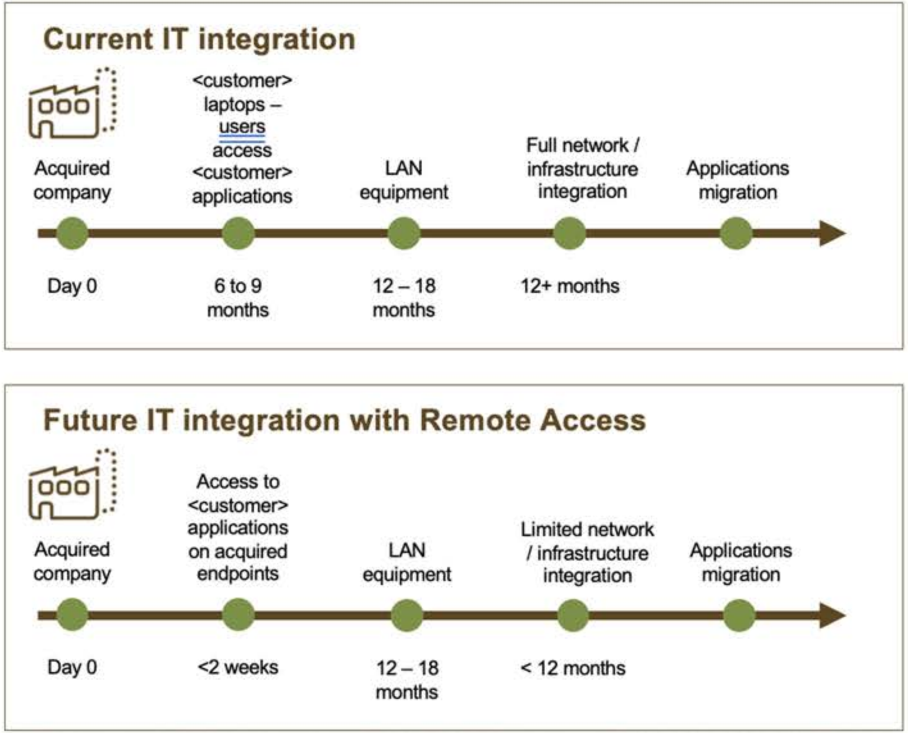
Security Posture Assessment – Question 1-4

Future state refers to Internet & Private Access for full population

#	Capability	Question	Answer Choices	Current (answer #)	Future (answer #)
1	Performing Full SSL Inspection	What is your capability on SSL inspection?	1 The organization doesn't have any SSL capability. 2 SSL inspection is done for on-site traffic. 3 SSL inspection is applied on most of the traffic. 4 SSL inspection is applied on every traffic (Server traffic+M365).	1	3
2	Downloading attachments to Sandbox	How much of your email attachments and browsing downloads are Sandboxed?	1 None to minimal traffic (web) is sandboxed. 2 Web traffic are partially sandboxed. 3 Web traffic are both protected by a moderate sandboxing control. 4 Web traffic are sandboxed and there is a tested process to handle malicious files/links download.	1	4
3	Cloud-Effect - Instantly Shared Protections	How is your current Web Proxy solution dealing with Updates?	1 The Proxy Solution is an on-premise solution with limited signature updates for IOC feed. IPS updates and URL Category are monthly updated. 2 The Proxy Solution is delivered with a Cloud-based solution - with minutes Signatures updates, IOC feed, IPS updates. 3 The organization use a Cloud Proxy Solution with minutes updates and AI/ML capability (to classify any Miscellaneous URL into a category). 4 The Cloud Web browsing Solution is receiving minutes updates and ingesting customer specific IOC via API.	1	4
4	Secure Remote User Access	How your users are accessing your Applications?	1 VPN enables the access to a trusted zone, which gives access to internal and SaaS Applications (M365, ServiceNow, Workday). 2 VPN and MFA give access to a trusted zone, from which internal and SaaS Applications are available. 3 VPN and MFA give access to a trusted zone, from which internal and SaaS Applications are, with Conditional Access such as device posture (Av or EDR running, internal device, Activity logs). 4 VPN and MFA give access to a trusted zone, from which internal and SaaS Applications are, with Conditional Access such as device posture. Applications are available through a cloud overlay platform compliant with ZTNA (Identity centric, Least privilege with Conditional access).	1	4

(4) Agility & Productivity

Sample: Day in a life scenario

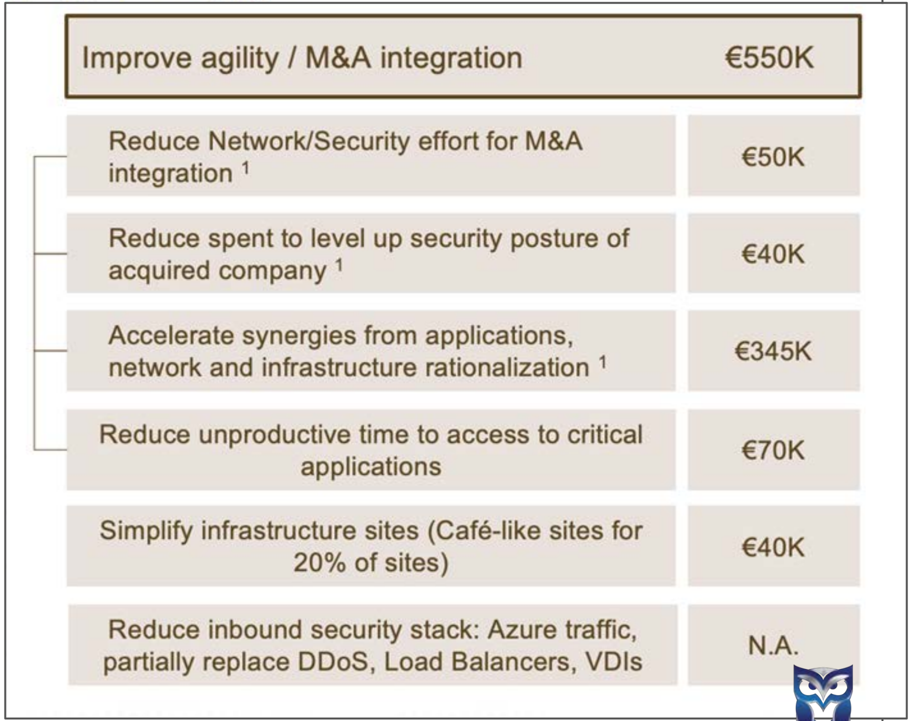


Current IT integration

Acquired company	<customer> laptops – users access <customer> applications	LAN equipment	Full network / infrastructure integration	Applications migration
Day 0	6 to 9 months	12 – 18 months	12+ months	

Future IT integration with Remote Access

Acquired company	Access to <customer> applications on acquired endpoints	LAN equipment	Limited network / infrastructure integration	Applications migration
Day 0	<2 weeks	12 – 18 months	< 12 months	



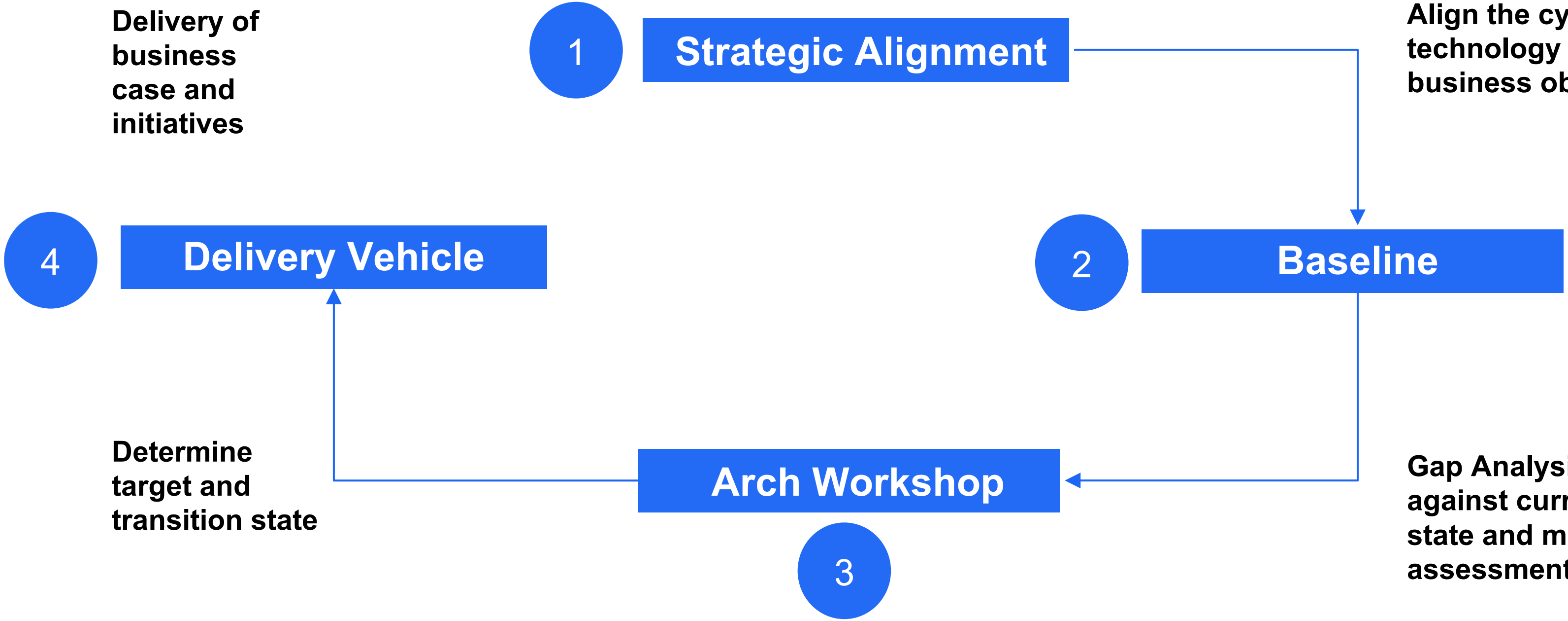
Improve agility / M&A integration	€550K
Reduce Network/Security effort for M&A integration [1]	€50K
Reduce spent to level up security posture of acquired company [1]	€40K
Accelerate synergies from applications, network and infrastructure rationalization [1]	€345K
Reduce unproductive time to access to critical applications	€70K
Simplify infrastructure sites (Café-like sites for 20% of sites)	€40K
Reduce inbound security stack: Azure traffic, partially replace DDoS, Load Balancers, VDIs	N.A.

IMPACT: 206 mins x 40% = 330 Hrs of extra Productivity per Employee per Year

Best Practices

CYBER ELITE

Approach and where to start on this journey?



Align the cyber and technology strategy to business objectives

Gap Analysis against current state and maturity assessment

Determine target and transition state

Delivery of business case and initiatives

Key Stakeholders

End User Compute

Cyber team

Infrastructure (networks)

Application Teams

Architecture (solution and enterprise)

CYBER ELITE

Zero Trust Roadmap Focus Areas

CYBER ELITE

Foundational

Define and understand all the actors

Asset, data, application and system management - Know what you need to protect

Understand the business processes and flow (determine high risk)

Identity and Access Management - right access at the right time (auth, IdP and provisioning)

Secure your ingress and egress points

Use discovery capabilities to map out the environment

User to Application connectivity use cases (including partners / suppliers)

Workload to third party, cloud, PaaS services

Policies based on criticality and risk and quick wins

Secure your workload to workload connectivity

Micro segmentation strategy - Logically group workloads.

Identify where are workloads are located low hanging fruit may be site to site.

Can workloads be differentiated.

Focus on high risk and critical assets.

End to End Monitoring and assessment

Threat Intelligence

Security Analytics

Asset and Vulnerability Management

Automation, deception and Response

Control measurement

Regulatory and industry reqs

Best Practices of Zero Trust for Successful Deployments

CYBER ELITE

Identity

Access is based on users roles and responsibilities.

Identity is managed through a centralised identity provider.

Device Identity, context and continual risk based checking is implemented.

Users can be anywhere and not tied to a network.

Workload

Workloads are logically grouped.

Workload locations are Identified and managed.

Workloads are logically grouped based on role and materiality.

Prioritise high risk and critical assets.

Network

Networks should only be used for transit.

Users should be independent to the network.

Controls are not network dependent.

Process

Only allow authorized processes to talk to each other.

All other connections are not allowed.

Automate controls and augment with internal know how.

End to End Monitoring and assessment

Summary

CYBER ELITE

So Why Zero Trust?

“Zero Trust deployments directly impact users, providing cyber teams with a great partnering opportunity in improving their experience”

Alignment to Core Security Principles	Least privilege, defence in depth, assume breach, continually verify
Reduces Risk	Reduces the attack surface, reduces data loss, reduces lateral movement and improves resilience
Provides and enables business agility and use cases	Cyber teams are more adaptable to change and future use cases
Learning from the past	Abstraction from the network to simplify the environment
Control harmonisation and reuse	Leveraging value from existing investments, identity / access engineering and full integration of capabilities
Build cyber champions	Offer a better user experience and engagement point
Cyber Operating Model Discussion	Is Zero Trust now more aligned with Cyber identity teams rather than the network?

CYBER ELITE

Resources

CYBER ELITE

Resources

- NIST 800-207 Standard Resource
  - https://csrc.nist.gov/publications/detail/sp/800-207/final
- CISA Zero Trust Maturity Model
  - https://www.cisa.gov/zero-trust-maturity-model
- zScaler – Seven Elements of Highly Successful Zero Trust Architecture
  - https://info.zscaler.com/resources-ebook-seven-elements-of-highly-successful-zta
- zScaler – Seven Pitfalls to Avoid when selecting an SSE Solution
  - https://www.zscaler.com/resources/ebooks/choosing-sse-solution.pdf

CYBER ELITE

CYBER ELITE

ติดตามข่าวสาร Cyber Elite ได้ที่

⌂ www.cyberelite.co

✉ mkt@cyberelite.co

LINE @cyberelite

☎ 094-480-4838

f Cyber Elite

in Cyber Elite

▶ Cyber Elite