

CyberRes

# Cyber Security and Cyber Resiliency: It's an Evolution

Stan Wisseman  
Chief Technologist  
[Stan.Wisseman@MicroFocus.com](mailto:Stan.Wisseman@MicroFocus.com)

# My evolving appreciation for Cyber Resilience...

**1984 – 87** NSA TCSEC product evaluator

Focused on Operating System security features/assurances

**1987 – 90** System Security engineer for US Air Force ground station

Trusted software development to extend TCB of B1 OS

Developed trusted code review process

**1990 – 93** Product Manager for Trusted Oracle7

**1993 – 2010** InfoSec Consulting

InfoSec Consultant at Trusted Information Systems

Director of InfoSec Consulting at Exodus Communications

Common Criteria Test Lab Manager at Arca Systems

Software Security Director at Cigital

Systems Security Engineering and Software Assurance at Booz Allen

**2010 – 14** Deputy CISO and then CISO at Fannie Mae

Information Security and Business Continuity programs

**Current** NA Chief Technologist for CyberRes



# Agenda

- Evolving Cybersecurity to Cyber Resilience
- Securing Identity Interactions with Zero Trust
- Securing Against Application Threats
- Enabling Data Privacy & Protection
- Accelerating Detection and Response
- Maturity Model and Road Ahead

# Cybersecurity is top of mind! But is it enough?



“88% of boards now view cybersecurity as a business risk... (Up 58% in last 5 Years)”

[Gartner – “6 Key Takeaways from the Gartner Board of Directors Survey” Oct 2021]

“Navigating current sources of disruption is a difficult undertaking, especially when they seem to have no end in sight: supply chain issues, cyberattacks, geo-political instability — let alone the pandemic.”

[Forbes – “Five Key Areas Of Focus For Resilience Management In 2022” Feb 2022]

“A focus on privacy laws, ransomware attacks, cyber-physical systems and board-level scrutiny are driving the priorities of security and risk leaders.”

[Gartner – “The Top 8 Cybersecurity Predictions for 2021-2022” Oct 2021]



# Going beyond Cybersecurity

- If an organization is targeted, eventually it will be compromised
- Organizations must be able to withstand attacks and continue to provide critical functions
- Resiliency must be built in – not tacked on

# Importance of Resilience

## Minimizing Impact

Cyber resilience is a shift to enable organizations to thrive despite:

Adversities | Crises | Volatility



# This is Cybersecurity...



Cyber Security is the “prevention of damage to, protection of, and restoration of computers (etc.) including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

## This is Cybersecurity...



## This is Cyber Resilience



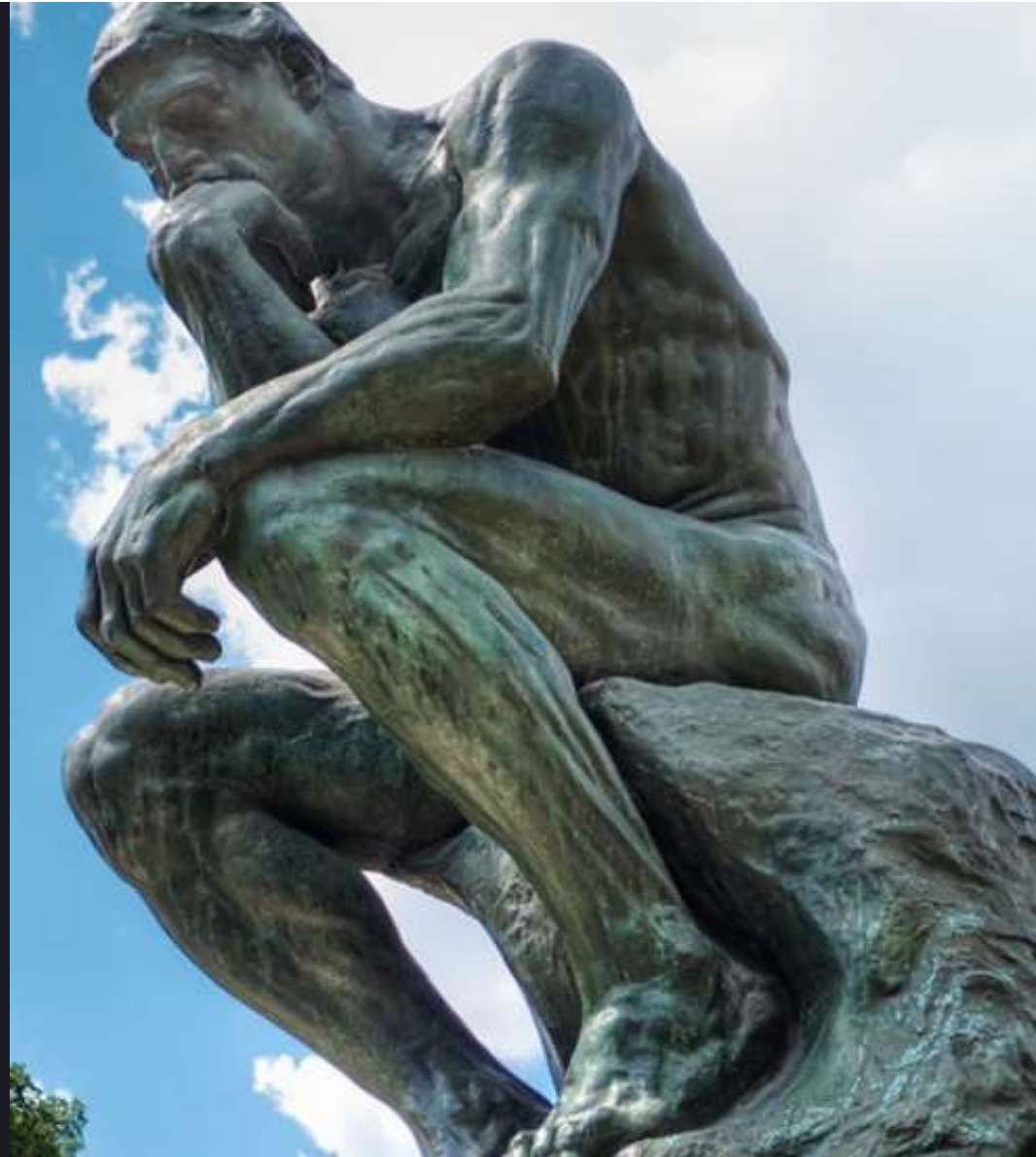
Cyber Resiliency is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”



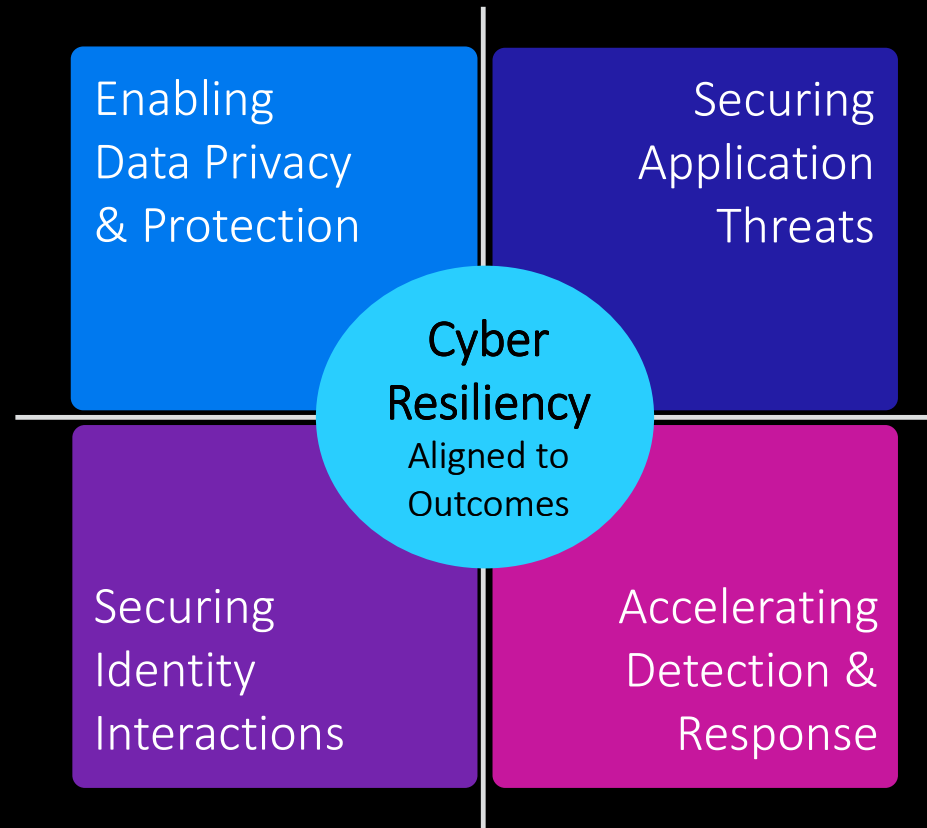


If cyber attacks are inevitable as well as flaws and weaknesses will always exist, leaders must assume incidents will be more likely and successful!

Therefore, Organizations must have a profound change in methodology and investment to implement cyber resilience.



# Organizational Outcomes Aligned to a Cyber Resilient Model



# Where to start? Identity is the New Perimeter

- Applications and data used to be protected inside of data centers.
- Data centers used to be behind locked doors, only accessible to IT professionals in white lab coats.
- With the move first to distributed offices then to road warriors and finally to remote workers, applications and data can no longer be kept in the data center
- Identities need to be authenticated and evaluated for every access – zero trust



# Securing Identity Interactions with Zero Trust



# How Organizations View Zero Trust

Top reasons for considering/implementing Zero Trust Security



**52.5%**

Zero Trust is more proactive than traditional approaches



**32.7%**

Zero Trust is the only way to combat sophisticated attacks

Source: Ericom 2021 Zero Trust Market Dynamics Survey

# What Does Zero Trust Mean?

## Basic Concept – Don't Assume Trust

- Need to maintain strict controls at every point of access
- Not trusting anyone or anything by default

## Follow the philosophy of least privilege

- Granting access to only what is needed
- Nothing more. Nothing less.

## Break the environment down into smaller security zones

- Minimizing the possible damage
- Slowing down the progress of a potential attack

## Verify identity at every step

- Guarantee a high level of assurance between security zones

# Components of a Zero Trust Architecture

## Least Privilege Access

- Grant only as much access as needed

## Micro-segmentation.

- Maintain separate security controls for each compartment of the environment
- Requires distributed management of these controls

## Multi-factor authentication (MFA)

- Require greater identity assurance based on current risk state

## API control and monitoring

- Manage programmatic access
- Control how many different devices and/or API's are trying to access resources.

## Adaptive

- Dynamically responding to current state in context of current environment and past activity

Visibility

Governance

Automation of security for continuous assessment

# Zero Trust Standards & Guidance in Government

The Federal Government has been preparing for the transition to a zero trust architecture for some time. Several agencies have published architectural models that can be helpful to other agencies:

- **NIST's SP 800-207, Zero Trust Architecture** provides a consensus definition and framework for the key tenets of zero trust architecture, while describing several different approaches to zero trust architecture that organizations with different risk postures and skillsets can adopt.  
Available at <https://csrc.nist.gov/publications/detail/sp/800-207/final>
- **NSA's Embracing Zero Trust** shows how deploying Zero Trust security principles can better position cybersecurity professionals to secure enterprise networks and sensitive data.  
Available at [https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI\\_EMBRACING\\_ZT\\_SECURITY\\_MODEL\\_UOO115131-21.PDF](https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF)
- **DoD's Zero Trust Reference Architecture** comprehensively describes potential security features and architectural controls that the Department plans to execute across its systems.  
Available at [https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT\\_RA\\_v1.1\(U\)\\_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)
- **CISA's Zero Trust Maturity Model** is a high-level overview of zero trust "pillars" that shows how agencies may progress to "Advanced" and "Optimal" states and describes how CISA service-offerings align to these pillars.  
Available at <https://www.cisa.gov/publication/zero-trust-maturity-model>
- **OMB's Federal Zero Trust Strategy**, the goal is to accelerate agencies toward a shared baseline of early zero trust maturity. Moving to a zero trust architecture will be a multi-year journey for agencies, and the federal government will learn and adjust as new technologies and practices emerge.  
Available at <https://zerotrust.cyber.gov/federal-zero-trust-strategy/>
- **GSA's Zero Trust Architecture Buyer's Guide** can help agencies identify GSA contract vehicles that offer products and services relevant to agency zero trust implementations.  
Available at [https://www.gsa.gov/cdnstatic/Zero\\_Trust\\_Architecture\\_Buyers\\_Guide\\_v11\\_20210610.pdf](https://www.gsa.gov/cdnstatic/Zero_Trust_Architecture_Buyers_Guide_v11_20210610.pdf)



# Zero Trust | a FRAMEWORK to achieve desired outcomes

Defined zero trust outcomes for government

## DoD

**Advanced**

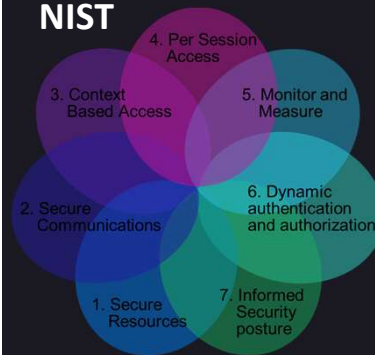
- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation
- Continuous and adaptive authentication and authorization
- User and Device Identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating Data Tags
- Advanced analytics enable automated and orchestrated threat detection

## NSA

**Advanced**

Deploy advanced protections and controls with robust analytics and orchestration

## NIST

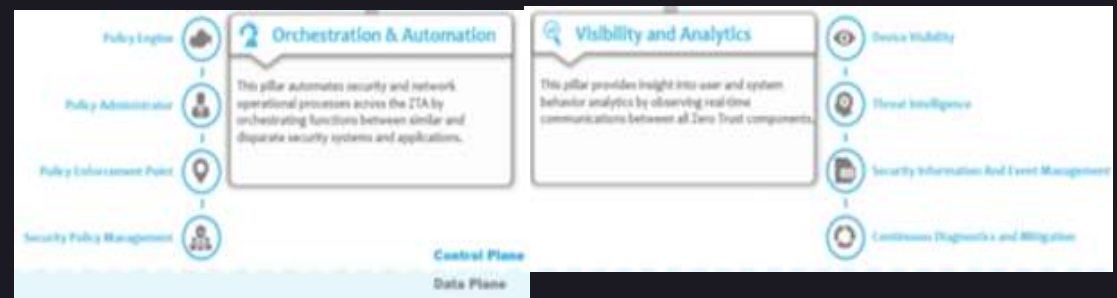


## CISA

Visibility and Analytics    Automation and Orchestration    Governance

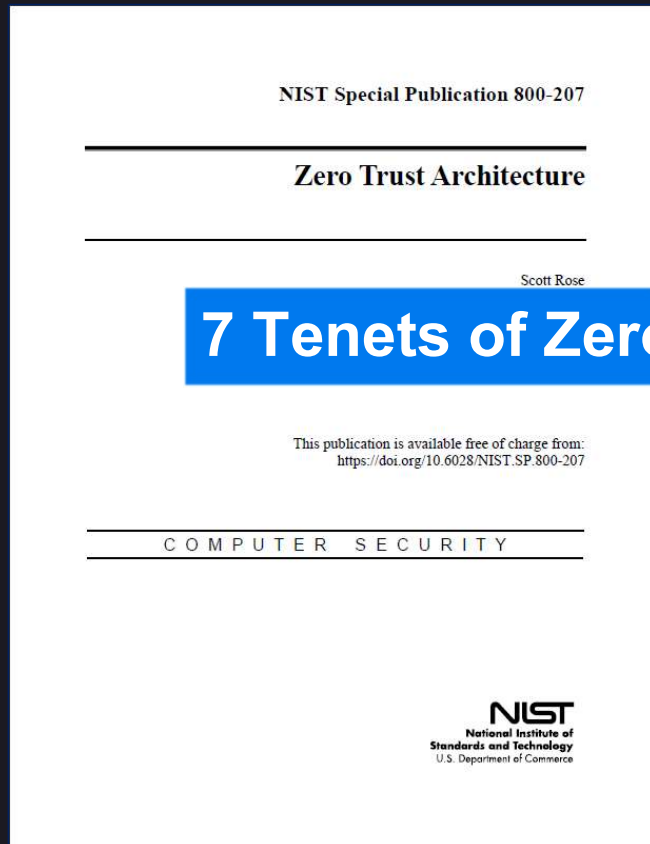
<ul style="list-style-type: none"> <li>• Continuous validation</li> <li>• Real time machine learning analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Constant device security monitor and validation</li> <li>• Data access depends on real-time risk analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Fully distributed ingress/egress micro-perimeters</li> <li>• Machine learning-based threat protection</li> <li>• All traffic is encrypted</li> </ul>	<ul style="list-style-type: none"> <li>• Access is authorized continuously</li> <li>• Strong integration into application workflow</li> </ul>	<ul style="list-style-type: none"> <li>• Dynamic support</li> <li>• All data is encrypted</li> </ul>
--------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

## GSA

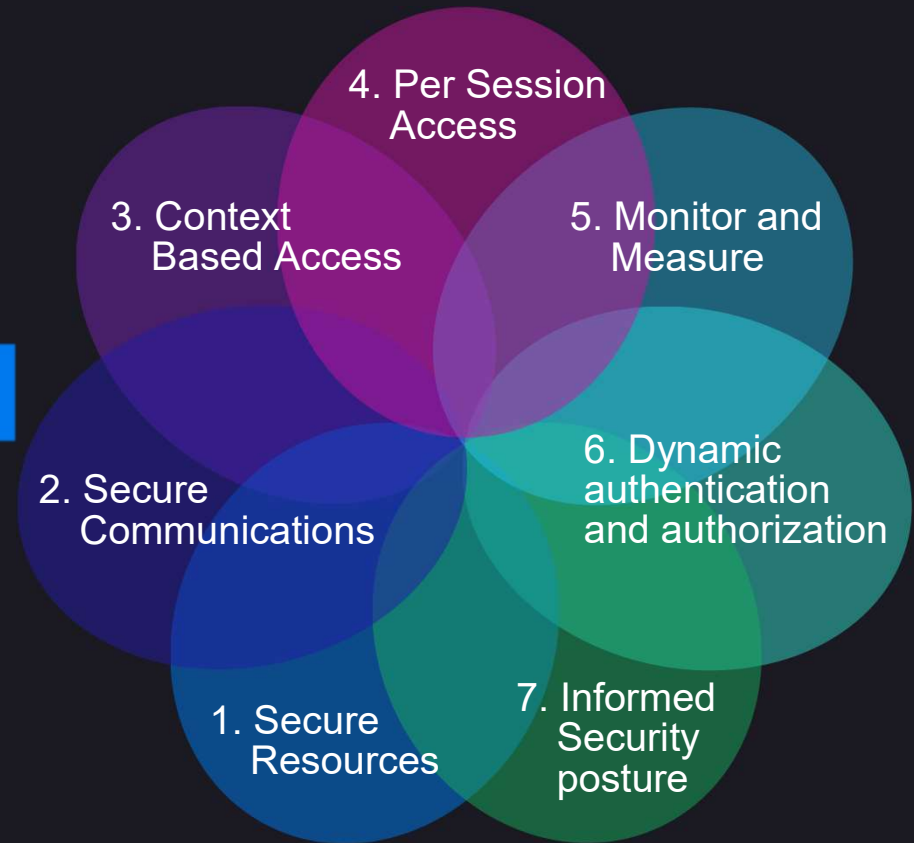


# NIST SP800-207 | Zero Trust Architecture

Released August 2020



## 7 Tenets of Zero Trust



<https://csrc.nist.gov/publications/detail/sp/800-207/final>

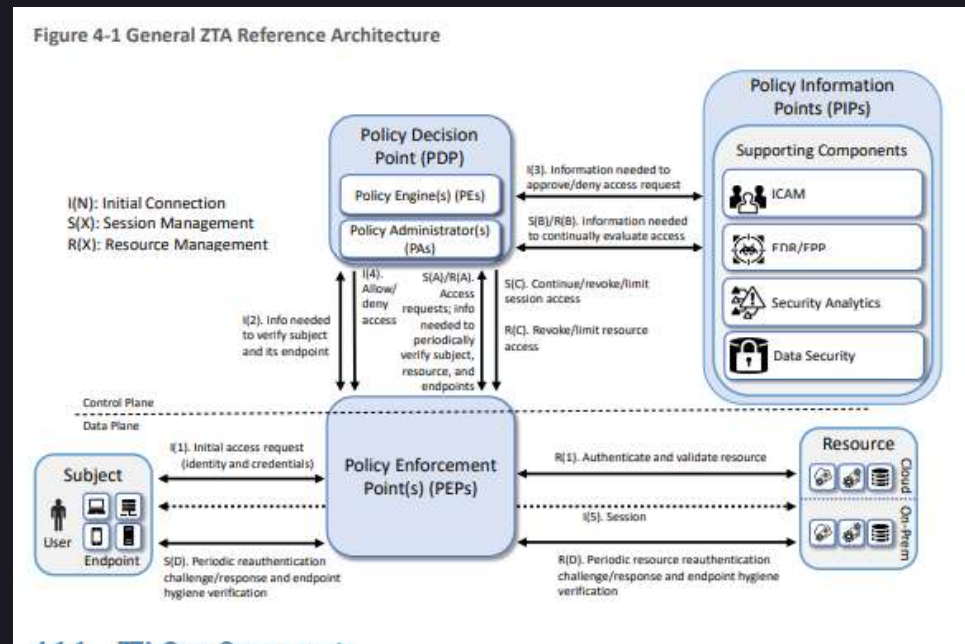
# NIST SP1800-35B | Implementing a Zero Trust Architecture

Preliminary Draft Released July 2022



**NIST SPECIAL PUBLICATION 1800-35B**  
**Implementing a Zero Trust Architecture**  
 Volume B:  
 Approach, Architecture, and Security Characteristics

<p><b>Oliver Borcher</b> Gema Howell Alper Kerman Scott Rose Murugiah Souppaya National Institute of Standards and Technology Rockville, MD</p>	<p><b>Jason Ajmo</b> Yann Fathina Dr. Parisa Grayeli Joseph Hunt Jason Harburt Neddi Iruchukuru Joshua Klossman Kenneth Sandlin Dissana Silvina Susan Symington Allen Ten The MITRE Corporation McLean, VA</p>	<p><b>Karen Scarfone</b> Scarfone Cybersecurity Clifton, VA</p>
<p><b>Michael Friedrich</b> Peter Gallagher Appgate Coral Gables, FL</p>	<p><b>Adam Cerini</b> Conrad Fernandes AWS (Amazon Web Services) Arlington, VA</p>	<p><b>Kyle Black</b> Sangeet Bandhwa Broadcom Software San Jose, CA</p>
<p><b>Peter Romness</b> Steve Vetter Cisco Hemdon, VA</p>	<p><b>Corey Bonnell</b> Dean Coolin Digicert Lehi, UT</p>	<p><b>Ryan Johnson</b> Dung Lam FS Seattle, WA</p>
<p><b>Tim Jones</b> Tim May Forescout San Jose, CA</p>	<p><b>Tim Knudsen</b> Google Cloud Mill Valley, CA</p>	<p><b>Mike Spisak</b> Harneet Singh IBM Armonk, NY</p>
<p><b>Corey Lund</b> Farhan Saifuddin Ivanti South Jordan, UT</p>	<p><b>Hashim Khan</b> Tim Lellmaster Lookout Reston, VA</p>	<p><b>Ken Durbin</b> Earl Matthews Mandiant Reston, VA</p>



# NSA Cybersecurity Information | Embracing Zero Trust

[https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI\\_EMBRACING\\_ZT\\_SECURITY\\_MODEL\\_UOO115131-21.PDF](https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF)

Released December 2020

## ZERO TRUST MATURITY

### WITHOUT ZERO TRUST

**Preparation**  
Initial discovery and assessment activities

### WITH ZERO TRUST

**Basic**  
Implement fundamental integrated capabilities

**Intermediate**  
Refine capability integration and further refine capabilities

**Advanced**  
Deploy advanced protections and controls with robust analytics and orchestration

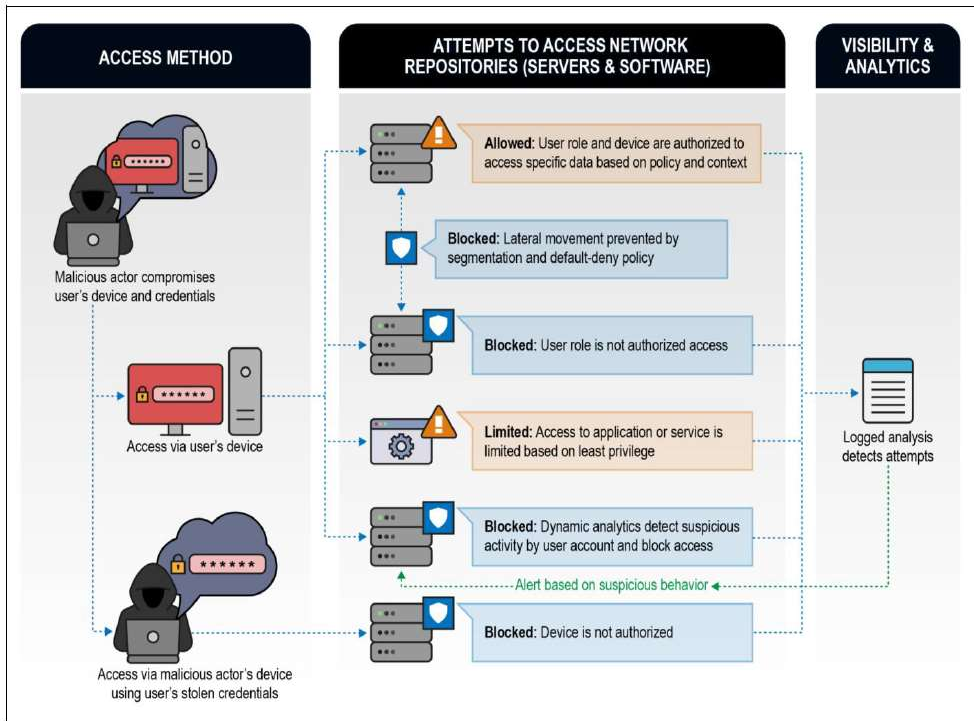
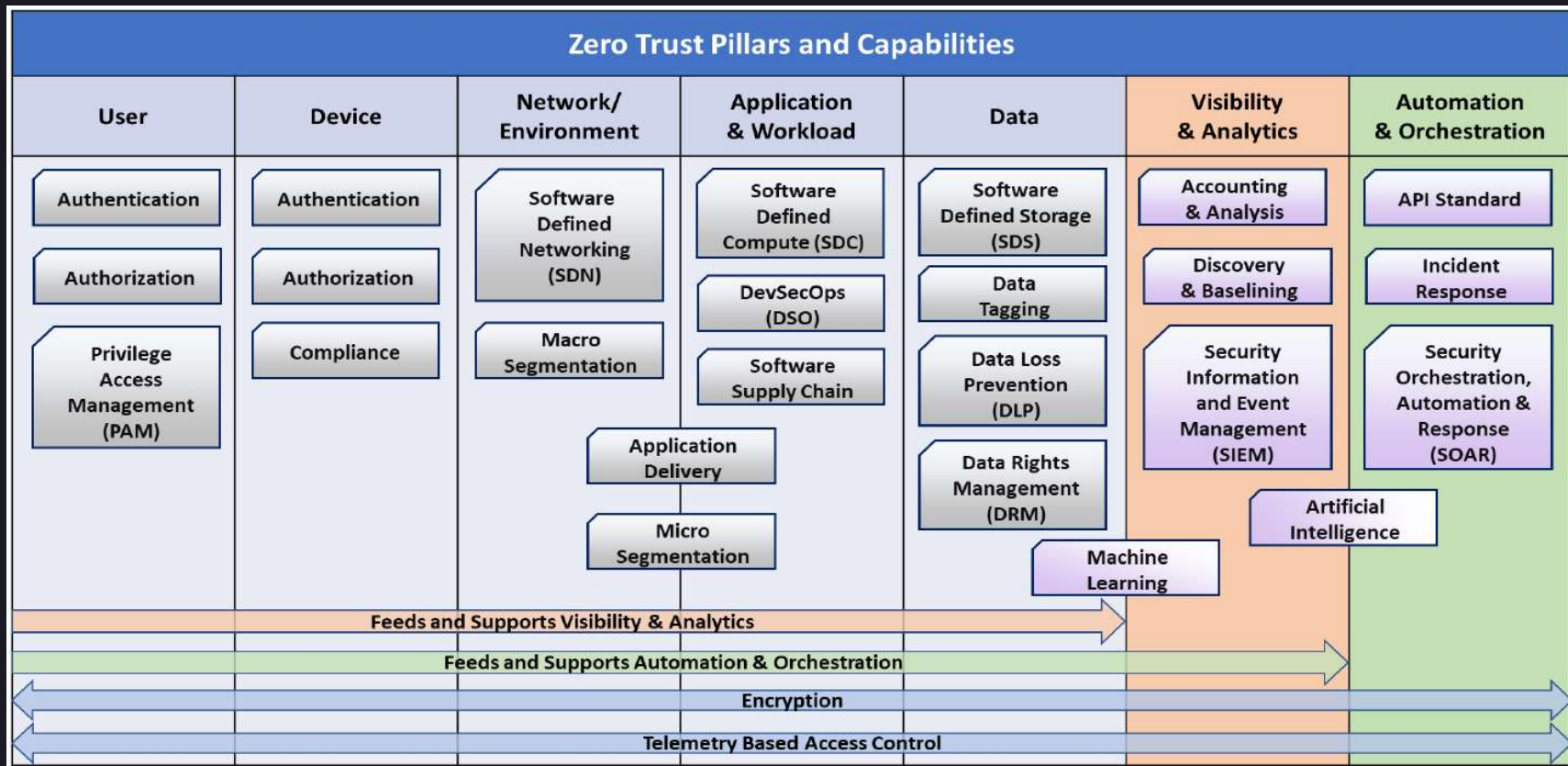


Figure 1: Example of Zero Trust remote exploitation scenarios where most attempts would have been successful in non-Zero Trust environments.

# DoD Zero Trust Architecture v1.0

[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT\\_RA\\_v1.1\(U\)\\_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)

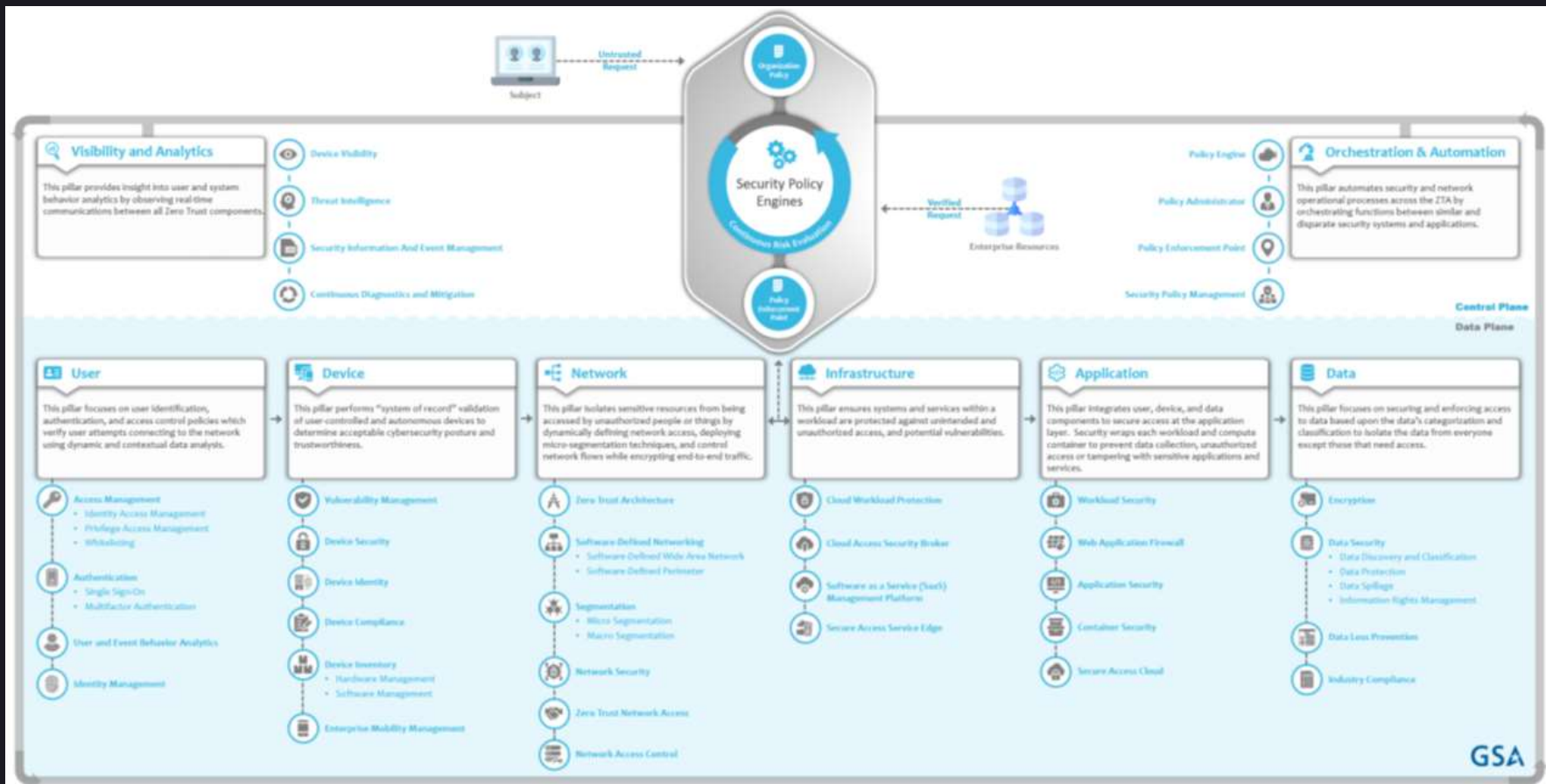
Released February 2021



# GSA Zero Trust Architecture Buyer Guide

[https://www.gsa.gov/cdnstatic/Zero Trust Architecture Buyers Guide v11 20210610.pdf](https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%2020210610.pdf)

Released September 2021



# CISA ZTA Maturity Model | Capabilities

<https://www.cisa.gov/publication/zero-trust-maturity-model>

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	<ul style="list-style-type: none"> <li>• Password or multifactor authentication (MFA)</li> <li>• Limited risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Limited visibility into compliance</li> <li>• Simple inventory</li> </ul>	<ul style="list-style-type: none"> <li>• Large macro-segmentation</li> <li>• Minimal internal or external traffic encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Access based on local authorization</li> <li>• Minimal integration with workflow</li> <li>• Some cloud accessibility</li> </ul>	<ul style="list-style-type: none"> <li>• Not well inventoried</li> <li>• Static control</li> <li>• Unencrypted</li> </ul>
	<p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p>				
	Advanced	<ul style="list-style-type: none"> <li>• MFA</li> <li>• Some identity federation with cloud and on-premises systems</li> </ul>	<ul style="list-style-type: none"> <li>• Compliance enforcement employed</li> <li>• Data access depends on device posture on first access</li> </ul>	<ul style="list-style-type: none"> <li>• Defined by ingress/egress micro-perimeters</li> <li>• Basic analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Access based on centralized authentication</li> <li>• Basic integration into application workflow</li> </ul>
<p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p>					
Optimal		<ul style="list-style-type: none"> <li>• Continuous validation</li> <li>• Real time machine learning analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Constant device security monitor and validation</li> <li>• Data access depends on real-time risk analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Fully distributed ingress/egress micro-perimeters</li> <li>• Machine learning-based threat protection</li> <li>• All traffic is encrypted</li> </ul>	<ul style="list-style-type: none"> <li>• Access is authorized continuously</li> <li>• Strong integration into application workflow</li> </ul>
	<p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p>				

# OMB Federal Zero Trust Strategy

<https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf>

*Released September 2021*

The Federal Zero Trust Strategy is published as *OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”*.

The goal of this strategy is to accelerate agencies toward a **shared baseline of early zero trust maturity**.



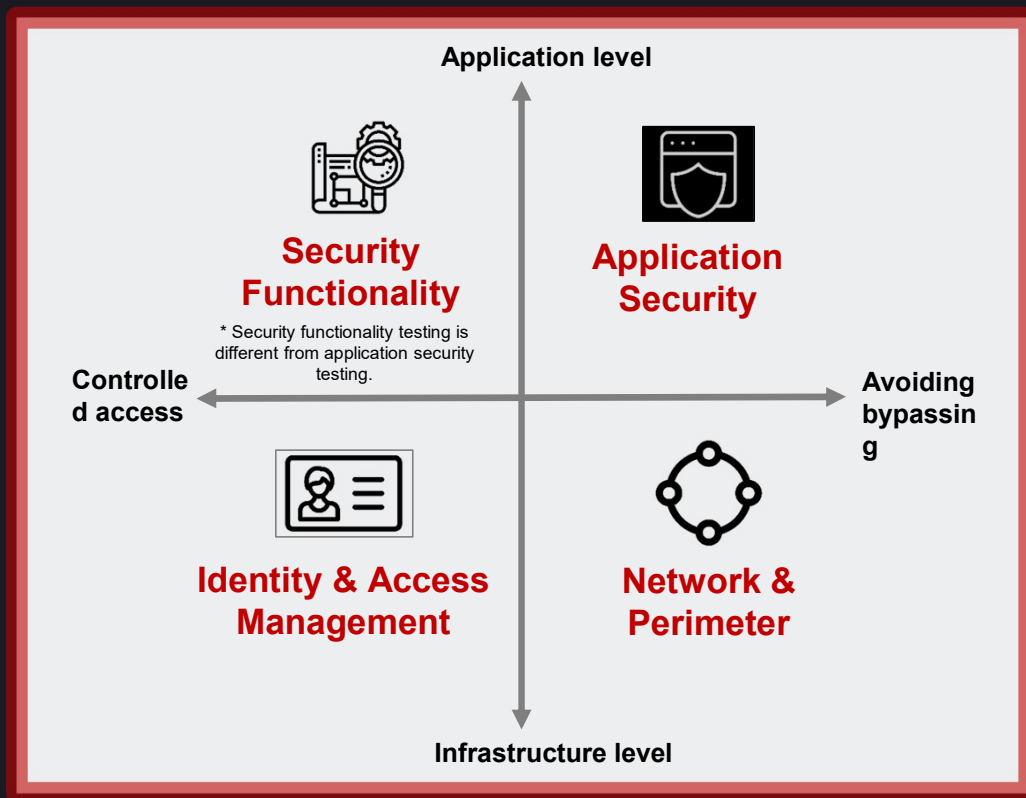


# Securing against application threats



# Attackers are moving from Infrastructure level to App level

Application layer attacks are perceived as normal traffic and pass through network, perimeter, data and endpoint security systems.



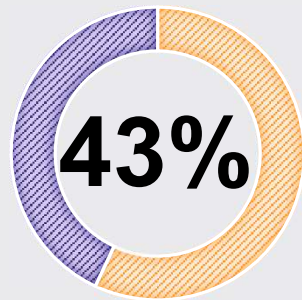
## Application security

- Not mature; lack of developer training
- Growing attack surface: more applications, more connected to the Internet
- Accelerating releases reduce time available for security

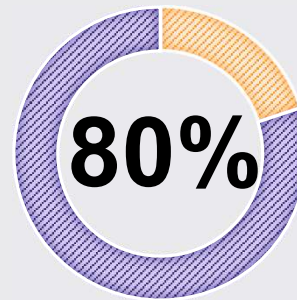
## Infrastructure security

- Highly mature
- Substantial investments in place
- Systems are more secure out-of-the-box than ever

# The Complexity of Software and Frequency of Releases Continues to Increase



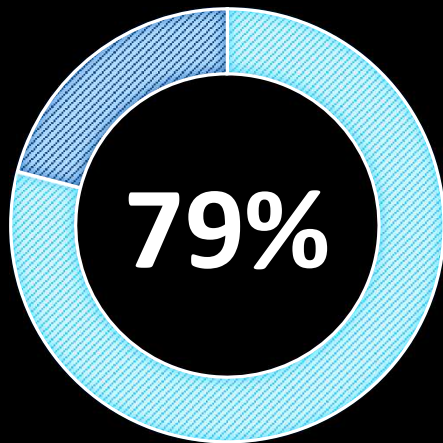
Of organizations release once per week or more



Of application code comes from open source libraries

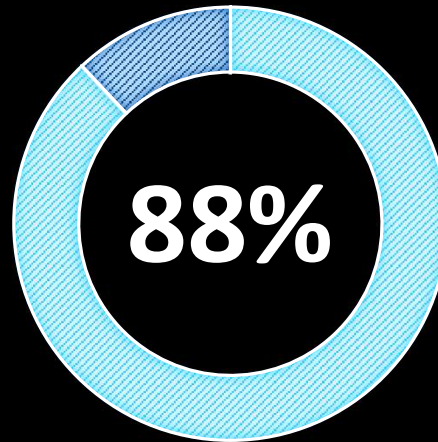
# As a result, most applications have security issues!

Source: "2019 Application Security Risk Report" by the Fortify Software Security Research team



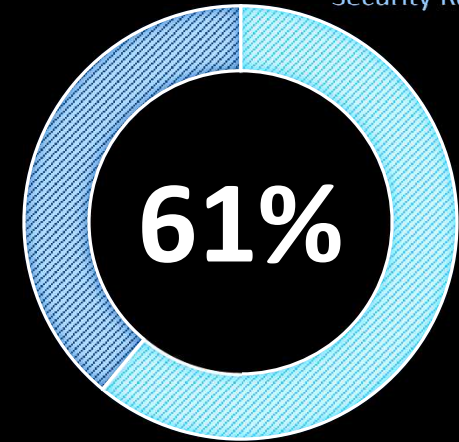
**of web apps**

have at least one critical or high severity issue



**of mobile apps**

have at least one critical or high severity issue



**of apps**

have critical or high vulnerabilities not covered by OWASP Top 10

**"Gartner predicts that by 2022, API attacks will become the most-frequent attack vector."**

[API Security: Protect your APIs from Attacks and Data Breaches](#)

# Software Supply Chain Threats are Increasing

“Supply chain attacks are increasing exponentially. In 2021 the world witnessed a 650% increase in software supply chain attacks.” (up from 430%)

[Sonatype “2021 State of the Software Supply Chain Report” Sept 2021]

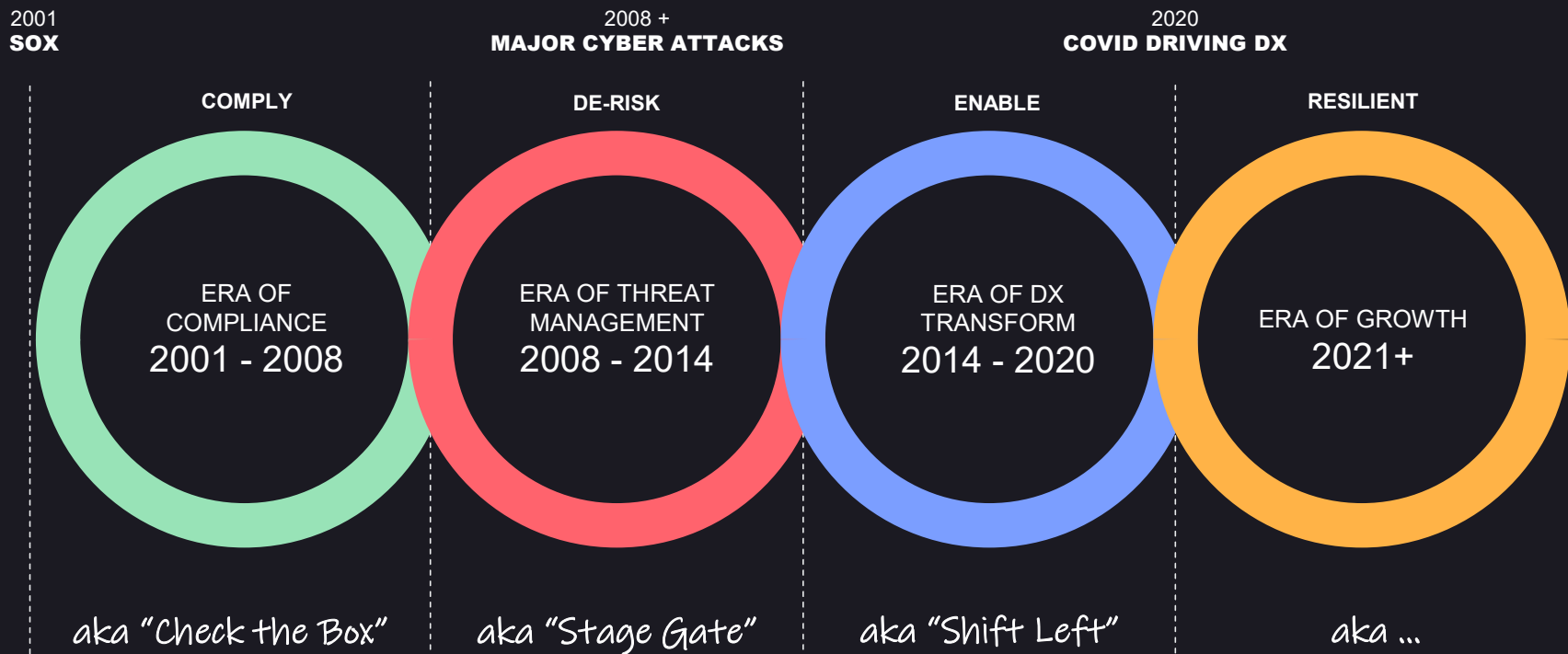
(Nation States) “have built the template for software supply chain attacks, particularly if they are able to compromise the commercial software code creation, distribution or code authentication processes.”

[Forbes “Software Supply Chains And Enterprise IoT Will Be Big Attack Targets In 2022” Jan 2022]



# AppSec's journey toward Cyber Resilience

Then, now, and in the future



# Time to put the Sec into DevOps -- DevSecOps



**Application  
security needs  
to be  
embedded  
earlier in the  
software  
development  
lifecycle**

## **Integration**

- Make application security available
- Embed application security into tools

## **Automation**

- Use automation to include security
- Track security defects as part of the SDLC

## **Agility**

- Provide insight & results fast
- Provide relevant issues with suggested fixes

# NIST SP 800-53r5

## (1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS

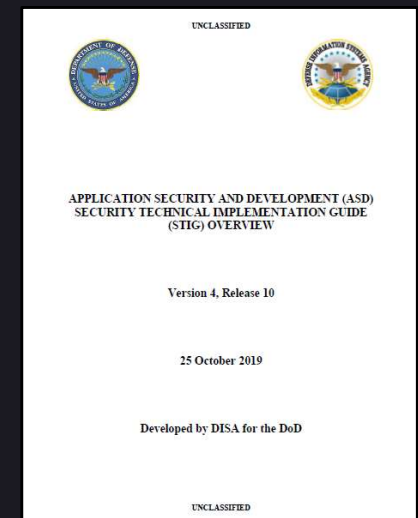
- **Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.**
- **Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported.** Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-11	Developer Security Testing and Evaluation		X		X	X
SA-11(1)	DEVELOPER SECURITY TESTING AND EVALUATION   STATIC CODE ANALYSIS		X			



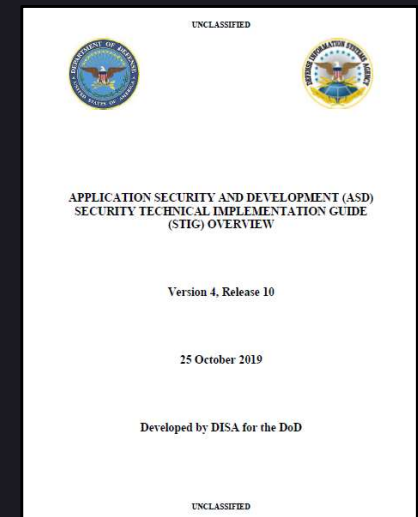
# DISA Application Security and Development STIG

- STIG ID: APSC-DV-001460
- Title: An application vulnerability assessment must be conducted.
- **An application vulnerability assessment is a test conducted in order to identify weaknesses and security vulnerabilities that may exist within an application.** The testing must cover all aspects and components of the application architecture. If an application consists of a web server and a database, then both components must be tested for vulnerabilities to the fullest extent possible.
- Vulnerability assessment tests normally utilize a combination of specialized software called application vulnerability scanners as well as custom scripts and manual tests. In some instances, multiple tools are required in order to test all aspects of application features, functions and architecture. The vulnerability scanner is typically configured to communicate with the application through the user interface or via an applications communication port. In addition to using automated tools, manual tests conducted from the OS console such as executing custom scripts or reviewing configuration settings for known vulnerabilities may also be included as part of the test..



# DISA Application Security and Development STIG

- STIG ID: APSC-DV-003170
- Title: An application code review must be performed on the application.
- Automated code review tools are to be used whenever reviewing application source code. These tools are often incorporated into Integrated Development Environments (IDE) so code reviews can be conducted during all stages of the development life cycle. **Periodically reviewing code during the development phase makes transition to a production environment easier as flaws are continually identified and addressed during the development phase rather than en masse at the end of the development effort.**



# Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e

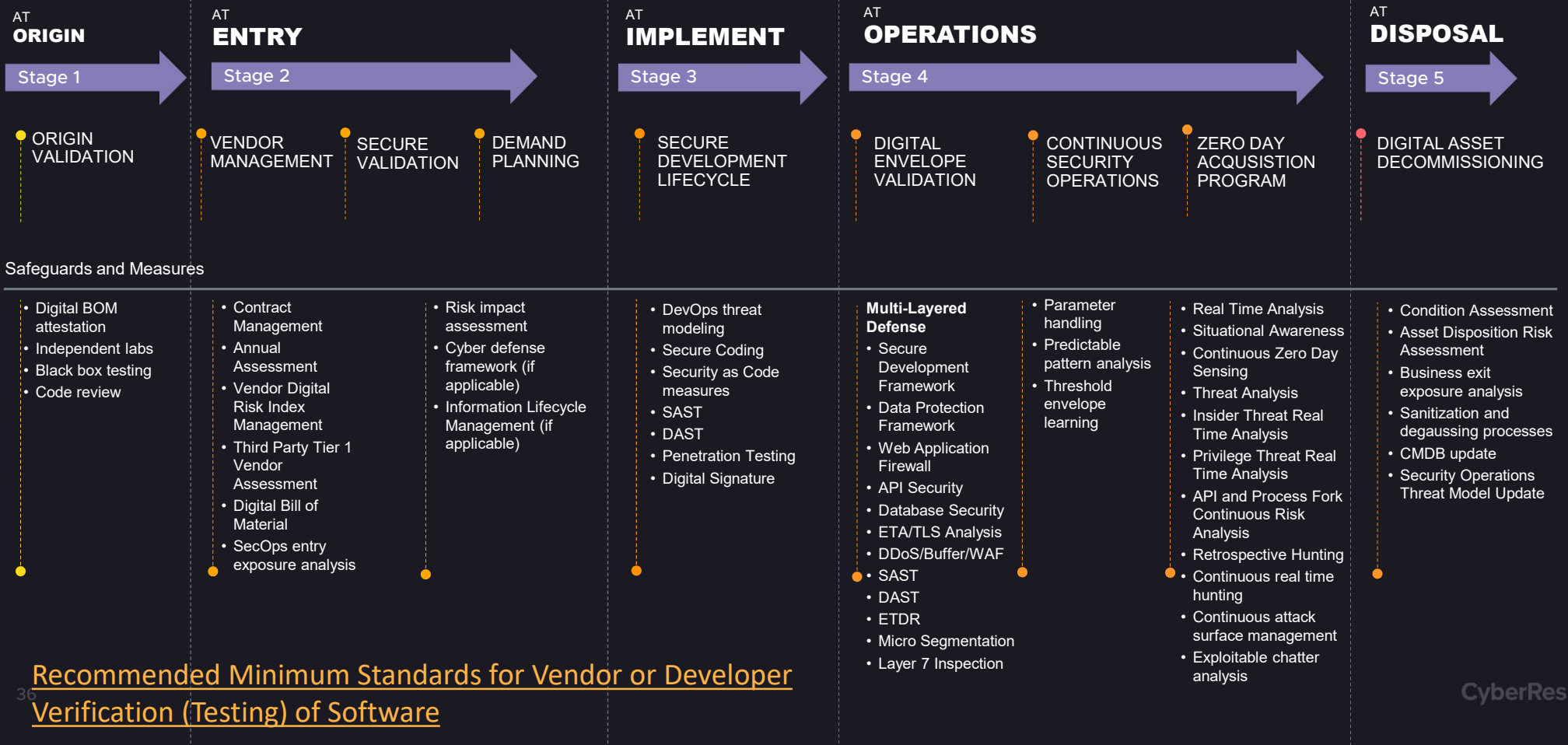
- EO 14028 emphasizes that “the security of software used by the Federal Government is vital to the Federal Government’s ability to perform its critical functions,” and “there is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended.” Accordingly, **secure software development practices should be integrated throughout software life cycles** for three reasons: 1) to reduce the number of vulnerabilities in released software, 2) to reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and 3) to address the root causes of vulnerabilities to prevent recurrences. [SP 800-218].

SSDF Practices Corresponding to EO 14028 Subsections		
EO 14028 Subsection	Subsection Summary (Refer to the next column for a complete list)	SSDF Practice and Task Reference Numbers
4e(i)	Have secure software development environments, including:	[See rows below]
<a href="#">4e(i)(A)</a>	administratively separate build environments;	PO.5.1
<a href="#">4e(i)(B)</a>	trust relationship auditing;	PO.5.1
<a href="#">4e(i)(C)</a>	multi-factor, risk-based authentication and conditional access;	PO.5.1, PO.5.2
<a href="#">4e(i)(D)</a>	minimized dependencies on enterprise products in development environments;	PO.5.1
<a href="#">4e(i)(E)</a>	data encryption; and	PO.5.2
<a href="#">4e(i)(F)</a>	operational monitoring and incident detection and response.	PO.3.2, PO.3.3, PO.5.1, PO.5.2

EO 14028 Subsection	Subsection Summary (Refer to the next column for a complete list)	SSDF Practice and Task Reference Numbers
<a href="#">4e(ii)</a>	Provide artifacts from 4e(i) upon request.	PO.3.2, PO.3.3, PO.5.1, PO.5.2
<a href="#">4e(iii)</a>	Maintain trusted source code supply chains.	PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4
<a href="#">4e(iv)</a>	Check software for vulnerabilities and remediate them.	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.2.1, RV.2.2, RV.3.3
<a href="#">4e(v)</a>	Provide artifacts from 4e(iii) and 4e(iv) upon request, and make a summary description of risks assessed and mitigated publicly available.	PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.1.2, PW.2.1, PW.7.2, PW.8.2, RV.2.2
<a href="#">4e(vi)</a>	Maintain provenance data for internal and 3 <sup>rd</sup> party components.	PO.1.3, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
<a href="#">4e(vii)</a>	Provide a software bill of materials (SBOM) for each product.	PS.3.2
<a href="#">4e(viii)</a>	Participate in a vulnerability disclosure program.	RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3
<a href="#">4e(ix)</a>	Attest to conformity with secure software development practices.	All practices and tasks consistent with a risk-based approach
<a href="#">4e(x)</a>	Attest to the integrity and provenance of open-source software components.	PS.2.1, PS.3.1, PS.3.2, PW.4.1, PW.4.4

# SECURING THE DIGITAL SUPPLY CHAIN

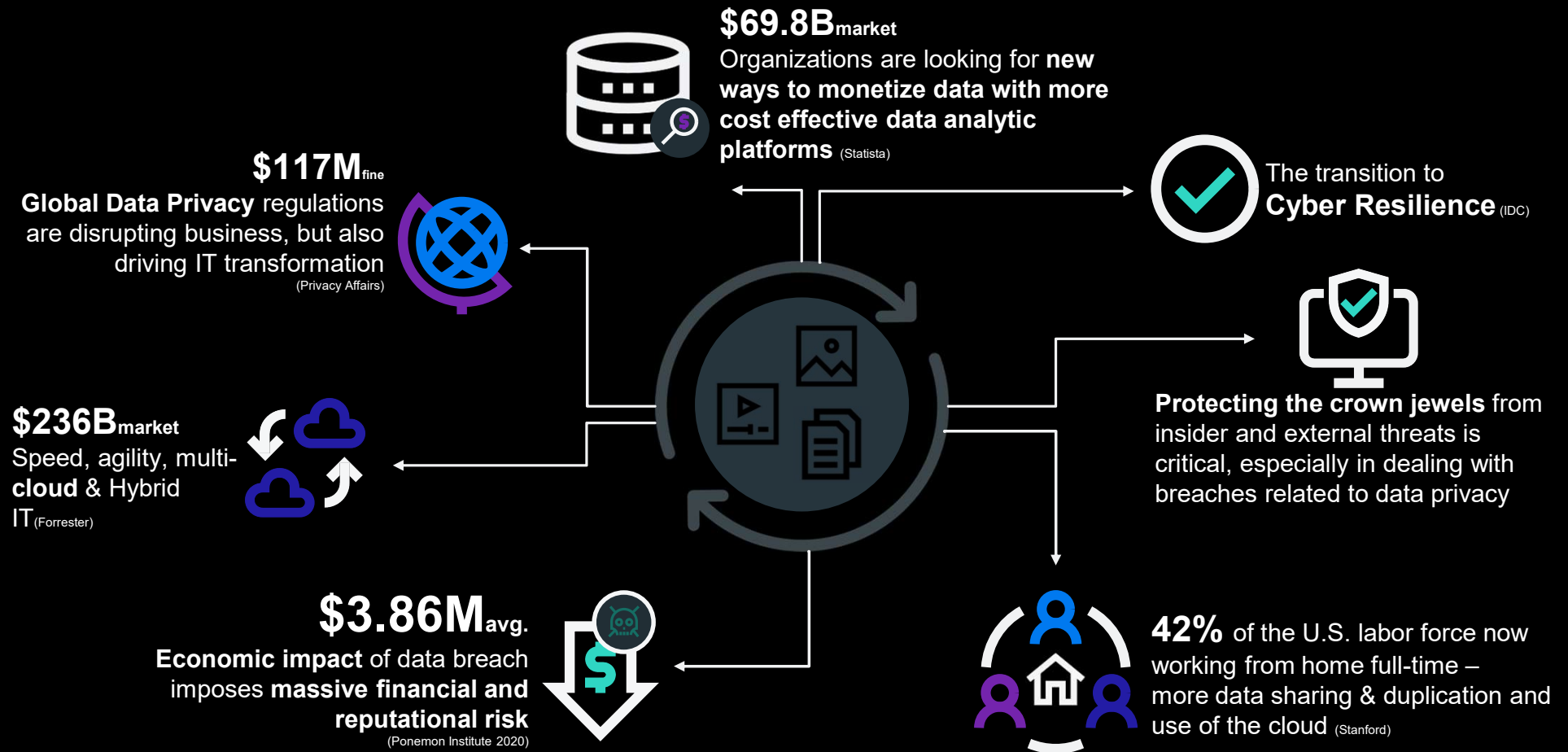
## SECURING END TO END SOFTWARE, DIGITAL AND INFORMATION SUPPLY CHAIN





# Enabling Data Privacy & Protection

# Enterprise Data Trends



You need a complete, reliable, adaptive, and automated, framework to navigate the new world of data protection and privacy.

# Establish the data privacy and protection framework



## Discover

**Know your data”**

You can't protect what you **don't understand**

You can't **protect everything** all the time



## Classify & Analyze

Gaining **insights** to all data is critical to **reducing risks**

Mastering the art of **deletion**, and **managing the data lifecycle**



## Manage & Protect

**Meaningful, proactive** approaches for protecting sensitive, high value, and personal data

**Protect data in use**, in motion, and at rest – wherever it is



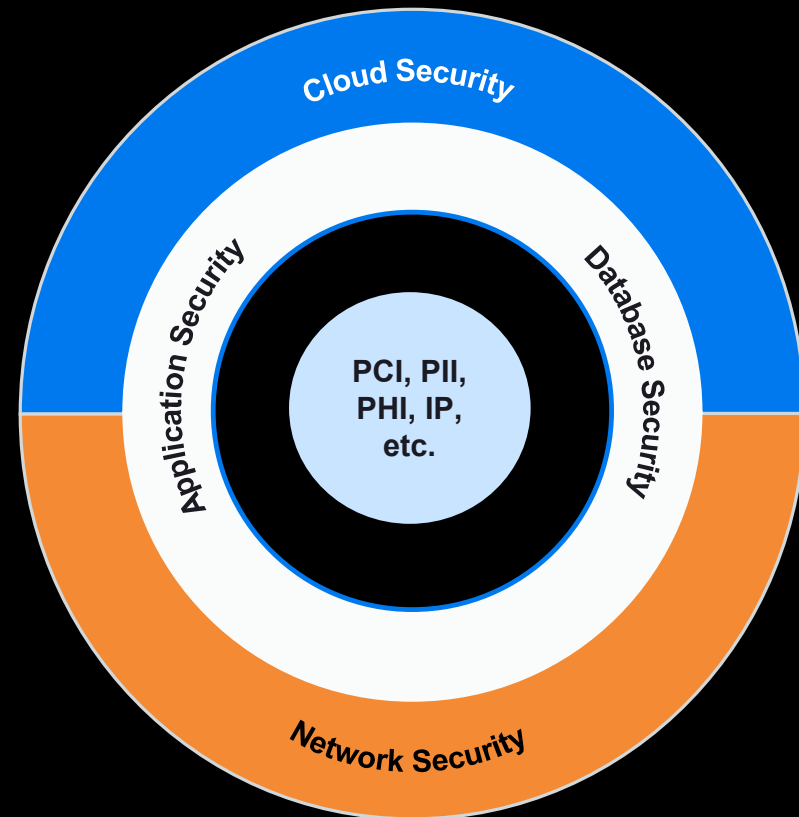
# Defense in depth, but start at the data layer

Work from the inside out

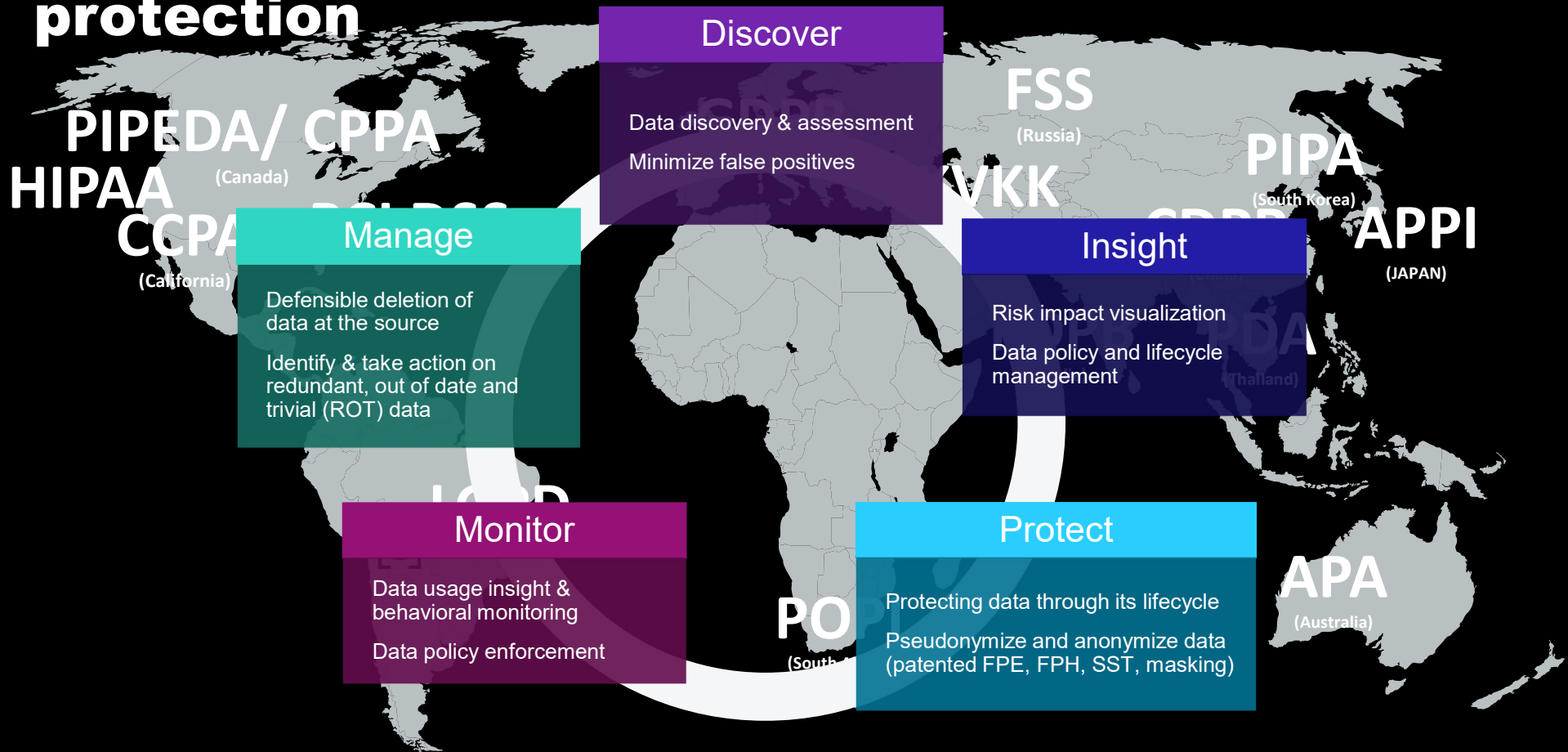
Close the gaps

Unify data security across hybrid IT

And beyond...



# Global framework addressing data privacy & protection



# Accelerating Detection and Response

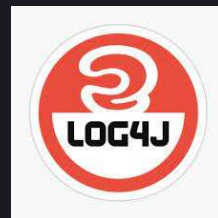


# Sit-Rep From the Data Breach Front

In 2021, we saw....

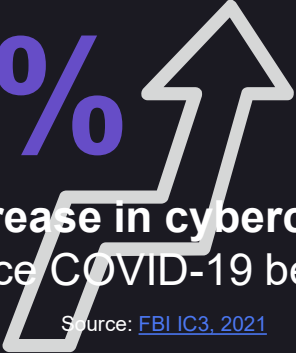
**4,145** DATA BREACHES

**22,770,000,000** EXPOSED RECORDS



# Rising Security Risks

**70%**  
Increase in cybercrime  
since COVID-19 began  
Source: [FBI IC3, 2021](#)



**93%**  
Of consumers would consider legal action  
against businesses if their personal data  
was stolen during a breach  
Source: [Gemalto Survey \(as reported by Tech Wire Asia\)](#)



**\$4.24  
million**  
Average total cost of a data breach  
Source: [Ponemon Institute, 2021](#)

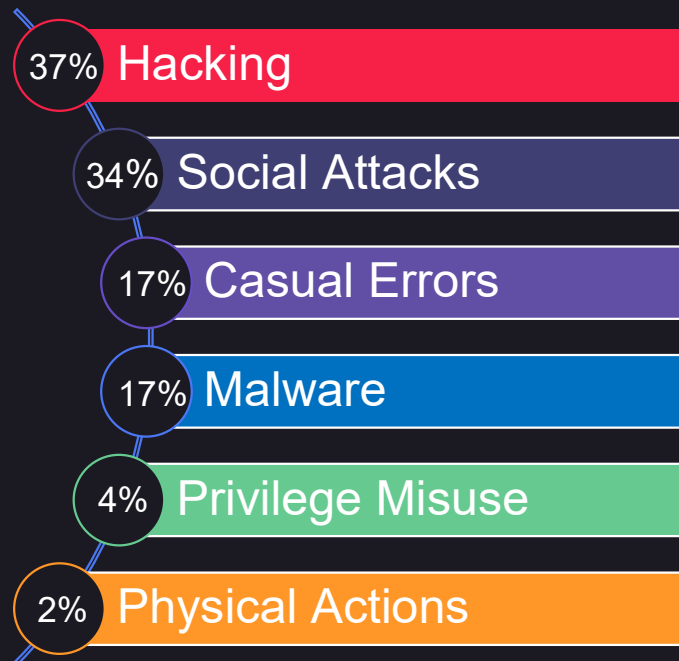


**287  
Days**  
Average time to identify  
and contain a breach  
Source: [Ponemon Institute, 2021](#)



# What Are We Up Against?

## TACTICS USED IN 2021 BREACHES



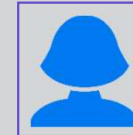
Cybercriminals  
Nation-state actors  
Malicious insiders  
Negligent insiders  
Partners  
Contractors



## MOST WANTED



The **bad guy** on the **outside**

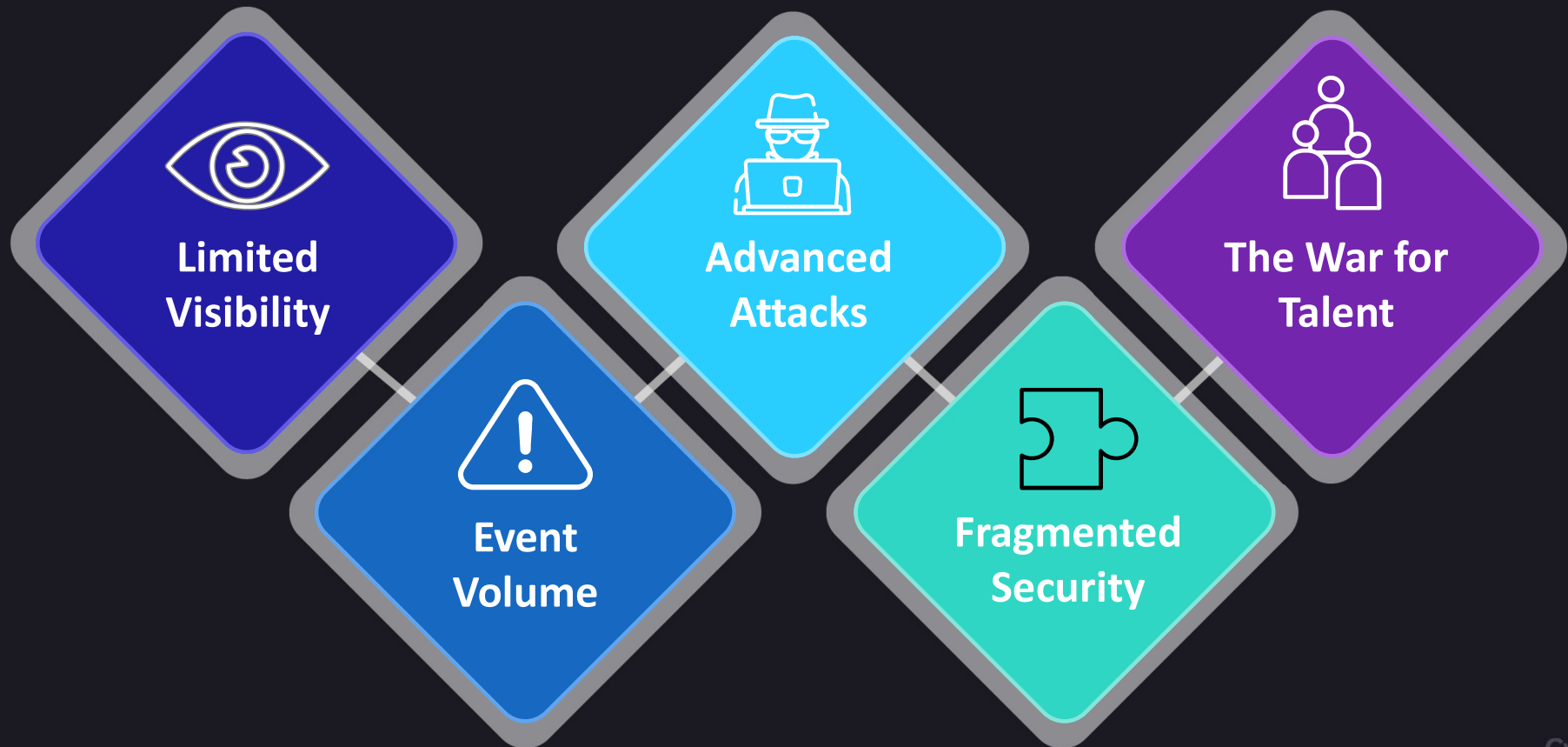


The **bad guy** on the **inside**



The **foolish guy** on the **inside**

# Why the Current SOC Can't Keep Up



# What is SOC Resilience?

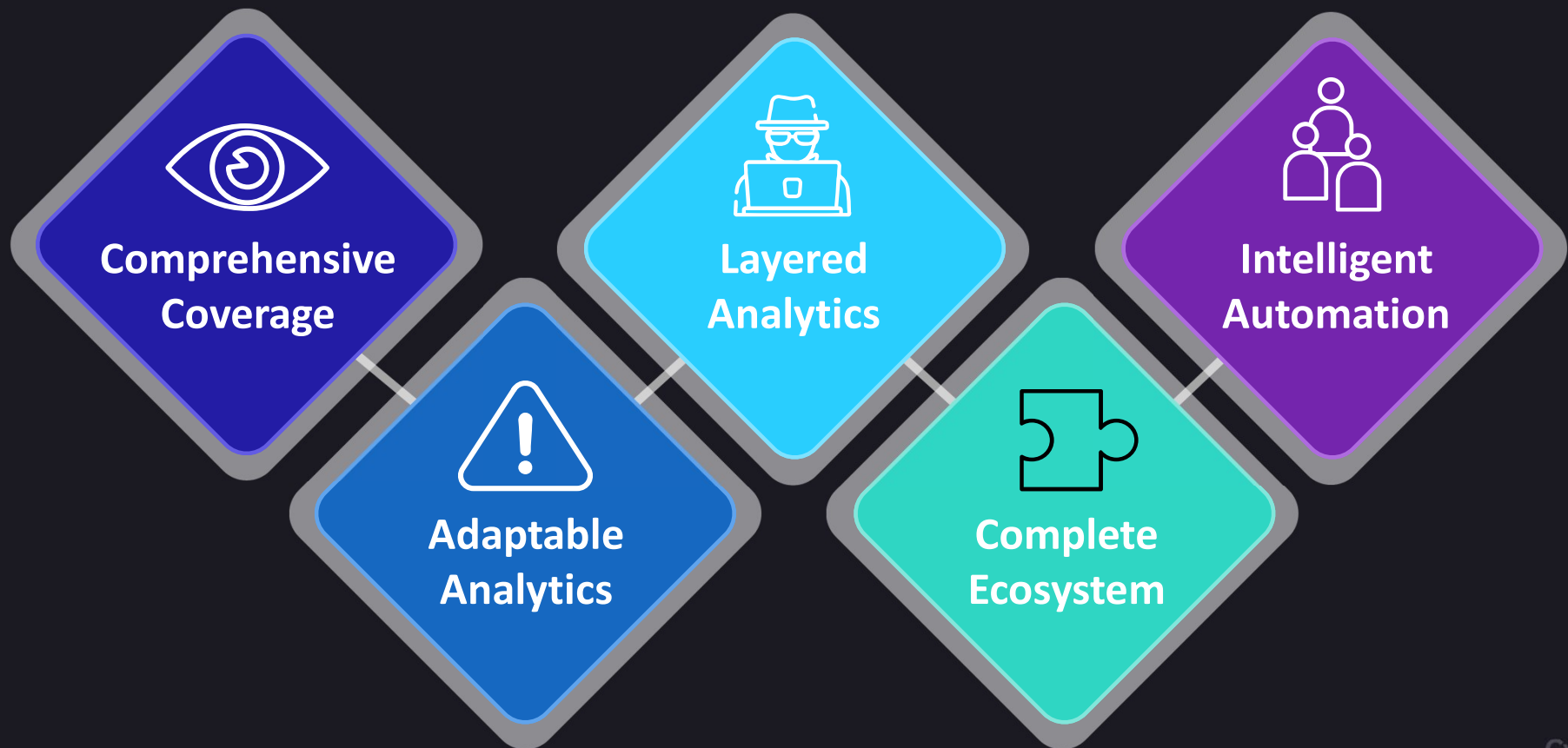
A SOC's ability to **adapt in the face of change and challenges** specifically those in the ever-evolving cybersecurity space, as well as its ability to **withstand and recover** from both accidental and deliberate actions against the SOC or against its organization's security stature.

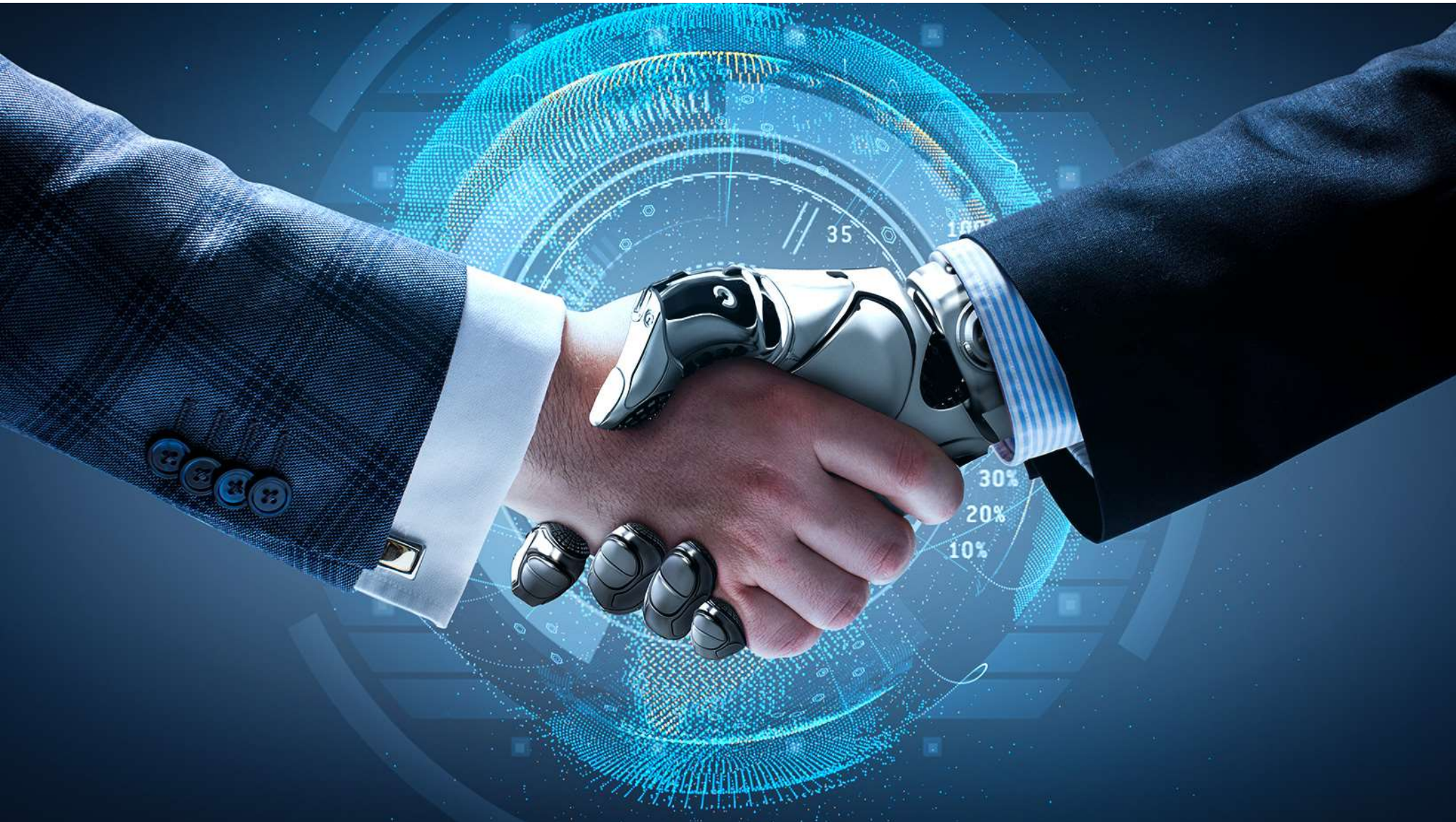
48 **Transitioning from reactive to proactive**





# What a Resilient SOC Needs





# Augmenting human intelligence with machine intelligence



**Unsupervised machine learning** means the engine can learn from the data and adapt intelligently.



**Automatic continuous online learning**, so that the engine never stops learning, and gets smarter over time.



**Embeddable into any ecosystem** so that different types of analysts can benefit from AI assistance where they do their jobs today.



**Discover the Unique Normal** of organizations so that the engine can develop detailed profiles of monitored entities, like a digital fingerprint.

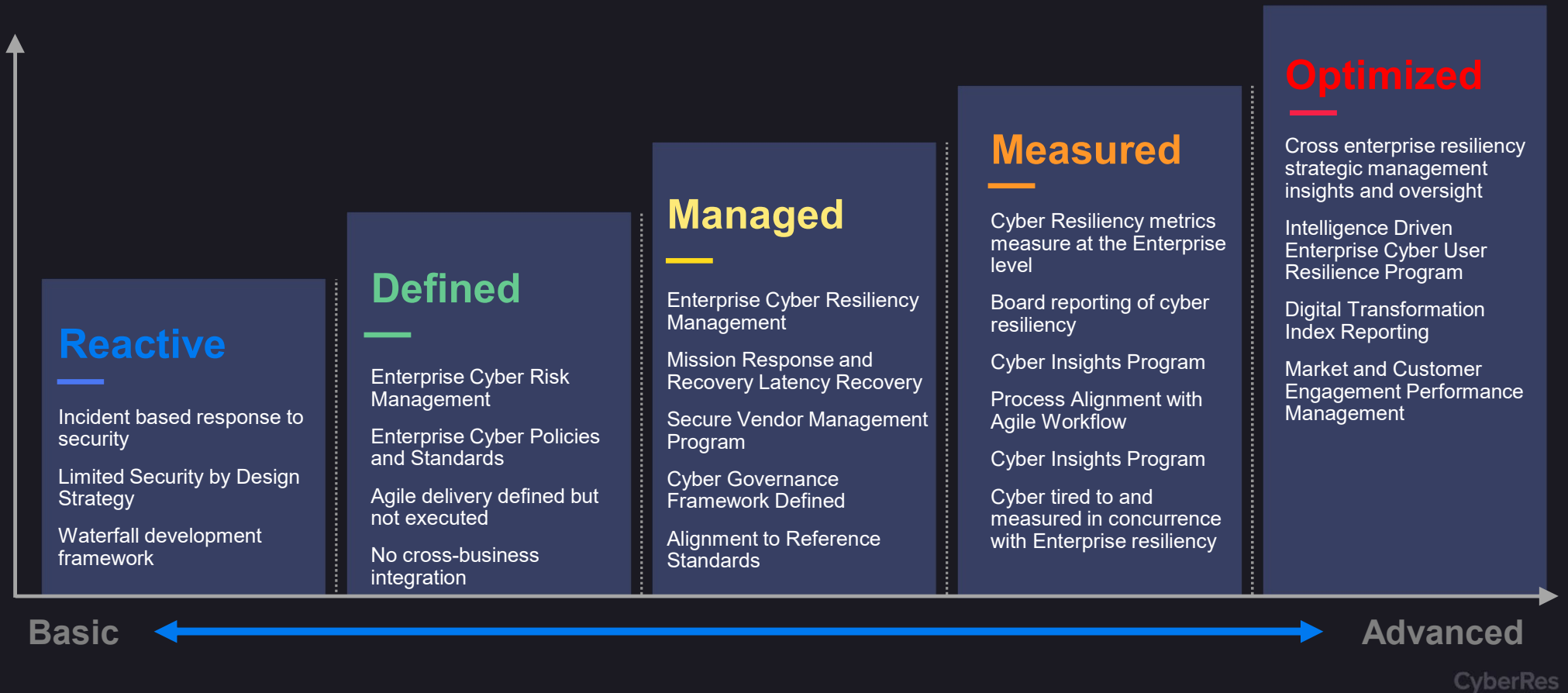


**Designed to be open and flexible**, to enable rapid use case addition and iteration.



**Deploy on-prem or in the cloud**, for one or multiple tenants, for the ultimate deployment flexibility.

# CyberRes Strategic Maturity Model



# The road ahead

Will depend on resilience like never before





# Cyber Resilience Focused Solution Portfolio

## Secure the Data

Discover, protect, and secure sensitive and high value data



Voltage



Fortify

## Secure the Application

Build secure software fast with a holistic application security platform



Intersect

## Secure the Identity

Secure access through a comprehensive identity and access management platform for all users, devices, things, and services



NetIQ



ArcSight

## Secure the Enterprise

Accelerate effective detection and response to known and unknown threats

Augment human intelligence  
with machine intelligence

**CyberRes**