VIGITRUST

Global Advisory Board

Emerging Trends that will challenge the security status quo

Emerging Trends that will challenge the security status quo

- No Uninviting the Third-party – Risk and reward for growing dependencies
- This Ain’t Your Father’s Crypto – Understanding the technology that we will rely upon
- Cybersecurity Moved Your Cheese – Adjustments to Corporate Mindset

VIGITRUST
Global Advisory Board

cloud security alliance®

"To promote the use of best practices for providing security assurance within Cloud Computing and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT
- GLOBAL, NOT-FOR-PROFIT ORGANIZATION
- RESEARCH AND EDUCATIONAL PROGRAMS
- CLOUD PROVIDER CERTIFICATION – CSA STAR
- USER CERTIFICATION – CERTIFICATE OF CLOUD SECURITY KNOWLEDGE (CCSK)
- THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD

OUR COMMUNITY

127,000+
INDIVIDUAL MEMBERS

105
CHAPTERS

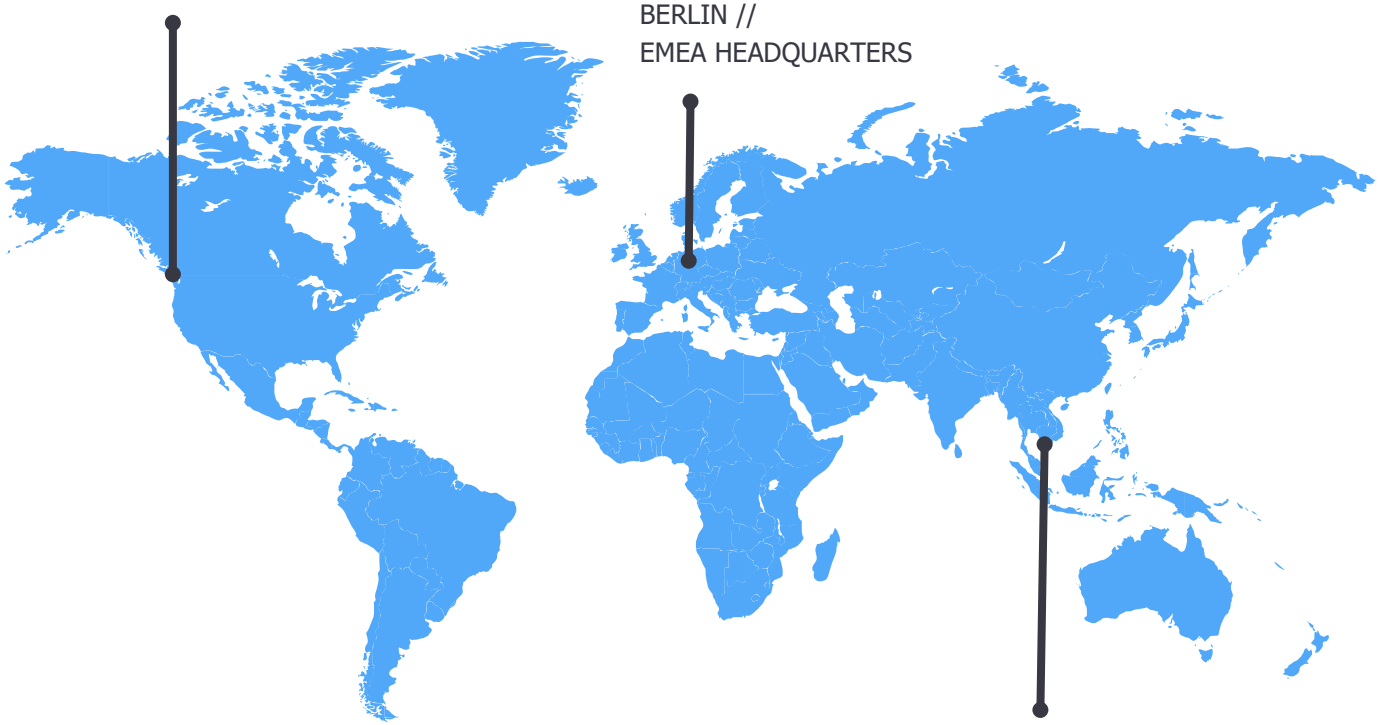
450+
CORPORATE MEMBERS

30+
ACTIVE WORKING GROUPS

2009
CSA FOUNDED

SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // EMEA HEADQUARTERS



SINGAPORE // ASIA PACIFIC HEADQUARTERS

Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

Third-Party Risk

- Open Source
- PayFac As a Service
- Growing MSP reliance

VIGITRUST
Global Advisory Board

RANSOMWARE IS THE KING OF CRIME

- Ransom Demands are Increasing
  - $5.3M average demand.
  - $570K average payout by 32% of victims

- 495M Ransomware attacks in first 9 months of 2021 (Sonicwall)
  - 90% of financial institution experienced attack in 2020

- 4/5 organizations were hit by a ransomware attack (Claroty x Forbes)

- CISO playbook now including ransomware payout in Incident Response Planning and cyber insurance

- **Prediction 1**: Ransomware will (nearly) eliminate all interest in financial data theft as a means for future fraudulent purposes

Open Source and Software Trends

Eenie, Meanie, Miney, Ow – only 3.3% of open source vulnerabilities are weaponized

But when they do….

Recent attacks have caused significant damage:

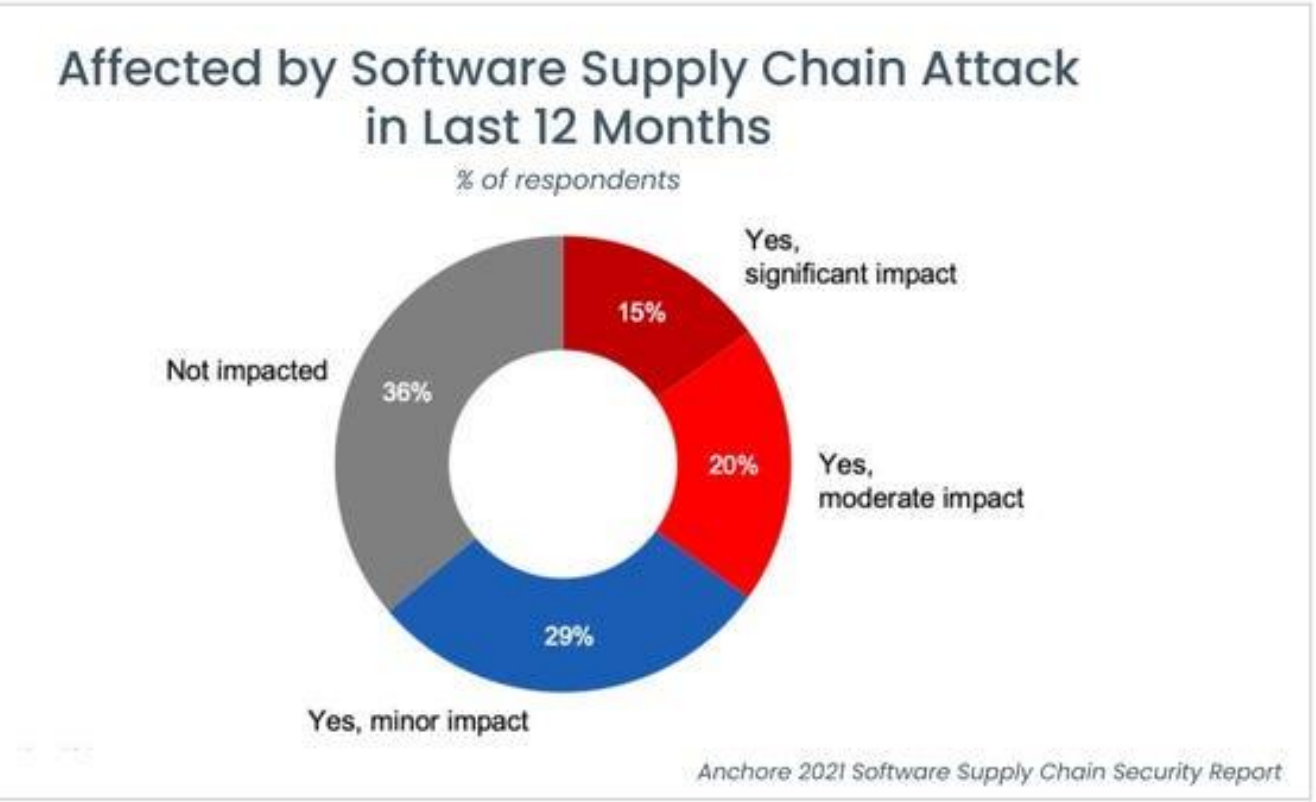
- Log4J/shell
- ApacheStruts

Update Agents being attacked

- SolarWinds Orion update packages
- ASUS LiveUpdate

2.2 Trillion open source packages downloaded in 2021

Software Supply Chain Challenges



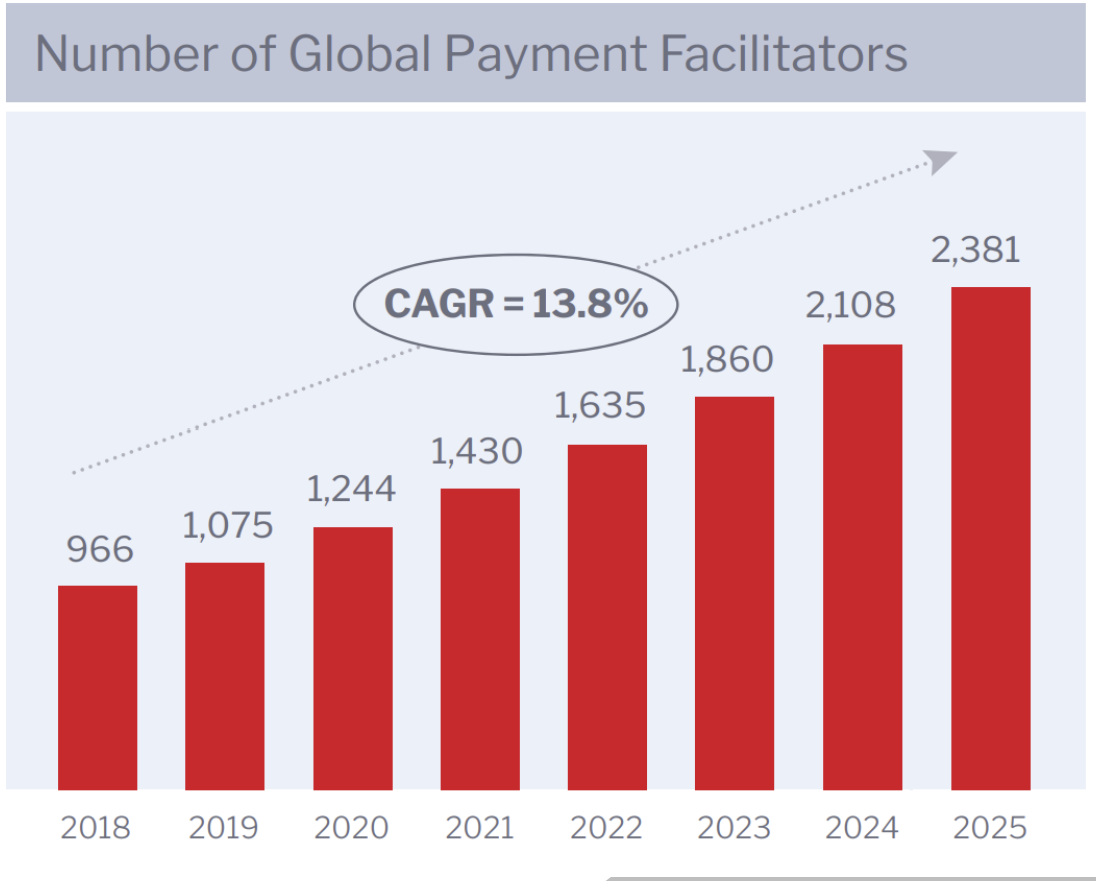
64% of security leaders would not know who to contact if open-source code was exploited.

- **Prediction 2:** Software Bill of Materials will become a standard practice and be influenced by regulation and other mandates

PayFac as a Service

Between 2018 and 2019, the GPV processed by all PFs worldwide increased from $699.11 billion (2018) to $928.64 billion (2019)

By 2025, the global GPV processed by payment facilitators is expected to reach over $4 trillion, experiencing a 28.4% compound annual growth rate (CAGR)



Data from *PAYMENT FACILITATOR GLOBAL OPPORTUNITY ANALYSIS AND INDUSTRY FORECAST 2018–2025 by Infinicept and AZ Payments Group*

PayFac as a SECURE Service

Two immediate areas of improvement include to minimize SW Developer access to sensitive data:

- authentication
- policy for Roles/Responsibilities

Prediction 3: PayFac as a Service will grow in popularity and undergo higher regulatory oversight

Eventually, there is a likely need for a PFaaS registry that is relevant for to those performing SaaS payments similar to the STAR Registry for Cloud Service Providers.

Migration to Cloud Services is Growing

Security and Compliance Rank as Top Challenges for Deploying Cloud-Native Apps

2021:

Software as a Service (SaaS) was largest market segment is at $149B and expected to reach $441B by 2027

– Research and Markets

2022:

75% of companies are focusing on developing cloud-native applications

- Tigera, *The State of Cloud-Native Security,* April, 2022

2025:

85% of organizations will embrace cloud-first & rely on cloud-native architectures/technologies to implement digital strategies

- Gartner Forecast, Nov 2021

Cloud (and other) Service Providers

Prediction 4: Critical/sensitive data will move a majority of operations to the cloud.

Prediction 5: Serverless will become a primary operational use and challenge to audit/monitor

1. Ensure security architecture aligns with business goals and objectives.
2. Develop and implement a security architecture framework.
3. Ensure the threat models are continuously kept up to date.
4. Bring continuous monitoring into the overall security posture.

Dependency on Crypto

- Digital Currency Trends
- Blockchain & Smart contracts
- Quantum

Digital Currency Trends

UK and US propose regulation to curb illicit use of Crypto

USDC Digital Coin ~$50B in circulation,
$3.1T digital-asset market
1.7 Trillion transferred on Chain

90% of the world's central banks have launched R&D efforts for CBDC, tracked in 91 countries

Rohit Chopra, CFPB – stablecoins not ready for consumer payments

Prediction 6: Energy consumption constraints will *eventually* be resolved, and cloud computing and API tools will link blockchains to create instantaneous, high-speed networks for digital national currency that will facilitate micropayments that can be more economically viable

Blockchain

Understanding blockchain technology and how it interacts with regulated sectors will be critical to securing your critical business services.

Value of blockchain is an unalterable record of transactions with end-to-end encryption, stored across a network of computers, with many nodes that act as trust agents, rather than one centralized attack target.

Privacy concerns may be better operationalized within DLT technology with the ability to anonymize data and require clear permissions to access.

Prediction 7: Mass adoption of smart contracts will occur sooner than other uses of blockchain

Blockchain is hard; Crypto Exchanges are easy

$3.18B lost in security breaches of a Crypto Exchange exploit; Additionl $7.7B scamming exploits

US Treasury sanctions SUEX, CHADEX for compliance controls to stop illicit activities

Misconfigurations have led to majority of data breaches:

- Unsecured data storage elements or containers
- Excessive permissions
- Default credentials and configuration settings left unchanged
- Standard security controls disabled

Prediction 8: More immediate oversight for consumer protection will be *attempted* for crypto exchanges

Y2Q: the Quantum Countdown

- Creating awareness to the future threat to all encrypted information
- Shor's Algorithm (asymmetric) and Grover's Algorithm (symmetric)
- CSA quantum countdown to April 14, 2030

Prediction 9: Capabilities to exploit will be available sooner than expected but less likely to be used

Quantum-Safe

Common strategies:

- Physical isolation
- Increasing symmetric key sizes
- Quantum Key Distribution (QKD)
- Use quantum-resistant cryptography
- Use hybrid solutions
- Quantum random number generators (QRNG)
- Using quantum-enabled defenses

Change in Cybersecurity Culture

- Zero Trust: Private and public sector support
- Boardroom Attention to Cybersecurity
- Trust of automation

Zero Trust and Privacy

ZERO TRUST DEFINITION & PRINCIPLES

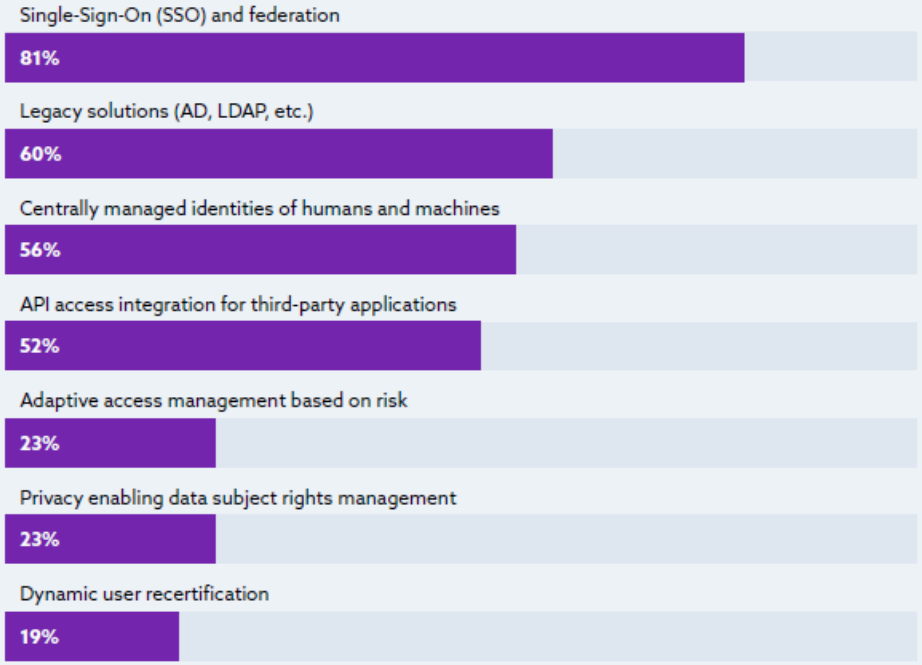
"Zero Trust is a ***philosophy*** of computer systems that holds no technologies, people or processes can be implicitly trusted in perpetuity and are thus prone to compromise. Therefore, risk-based strategies must be developed to ***build in*** appropriate measures to create the ***proportionate trust*** necessary for those systems."

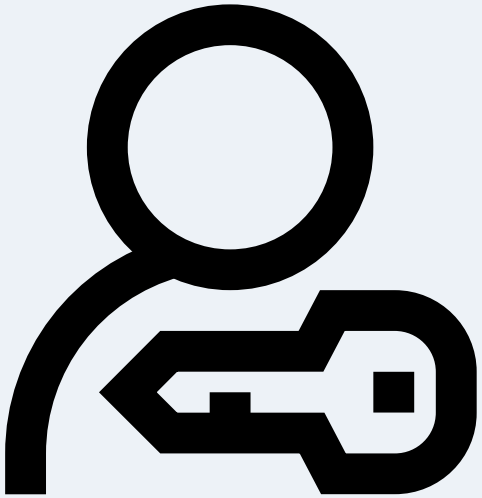
- Start from the key assets you want to protect. Design the system from the inside out around them.
- Trust no one and nothing, until validated and verified (make no assumptions, assume hostile environment).
- Enforce the need to know and least privilege access principles.
- Monitor (continuously…) what's happening.
- Change policies based on context.

ZERO TRUST

71% of organizations have a partial implementation or are planning to implement. **8%** of organizations have fully implemented zero trust

Methods for Managing Identity in Multi-Cloud





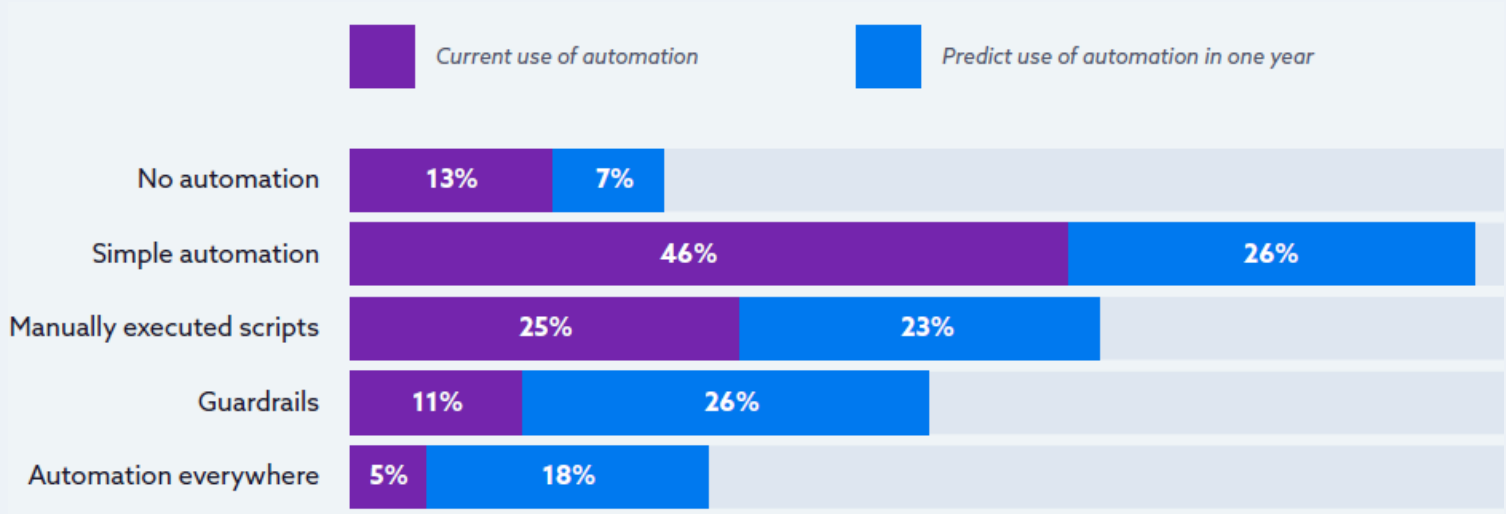
ZERO TRUST Advancement Center

- Common understanding of Zero Trust lacking
- Curation of CISA, NIST, Industry best practices
- Zero Trust Training Curriculum, Certificate of Zero Trust Knowledge (Q1 2023)
- Original research, tools & surveys
  - *Zero Trust as Security Philosophy* Whitepaper (June, RSA)
  - *CISO Perspectives & Progress in Deploying Zero Trust* Survey (June, RSA)
  - *Much more TBD*
- Zero Trust Online Summit (November)

Cybersecurity Coming to a Boardroom Near You

TRUST OF AUTOMATION AND ADOPTION

84% of organizations report having no automation or are still on the journey to use automation. Only **5%** of organizations report using automation everywhere. Lack of expertise was the top barrier to the use of auto-remediation insufficient or non-existent.



AUTOMATION AND AI BECOMING REALITY

Speed and Complexity of Environments necessitate adoption

Indicator Feeds, and good metrics will help create the right information to make better decisions

Prediction 10: Risk professionals will embrace automation sooner than later, if/when:

- Better understanding of technology
- Better curation of data
- Regulators provide public guidance

CSA Chapter

Chapters are made up of local security professionals who volunteer to increase cloud security awareness in their local community and provide outreach for CSA research, education, and training resources.

- Build cloud security awareness at the community level
- Participate in cloud security education and training locally
- Participate in CSA research and development
- Discuss cloud vulnerabilities and brainstorm solutions
- Free audit and compliance tools and programs
- Be a leader in the cloud security field

Conclusion

Ransomware and Privacy Challenges will Only Continue to Rise

Third-party risk is rapidly evolving and requires new approaches

Can’t dismiss the changes happening now that impacts the future of crypto

Security culture changes will be influenced by leaders around this room

VIGITRUST
Global Advisory Board