pactera EDGE

PACT.CLOUD-SECURITY AS AN SERVICE OFFERING'S

pactera EDGE

PACTERA EDGE SPECIALIZES IN DATA, INTELLIGENCE AND USER EXPERIENCE TO DELIVER INNOVATIVE PRODUCTS AND SOLUTIONS THAT TRANSFORM BUSINESSES

FACTS + FIGURES

12
Global Offices

5k +
Employees

100+
Fortune 500 Clients

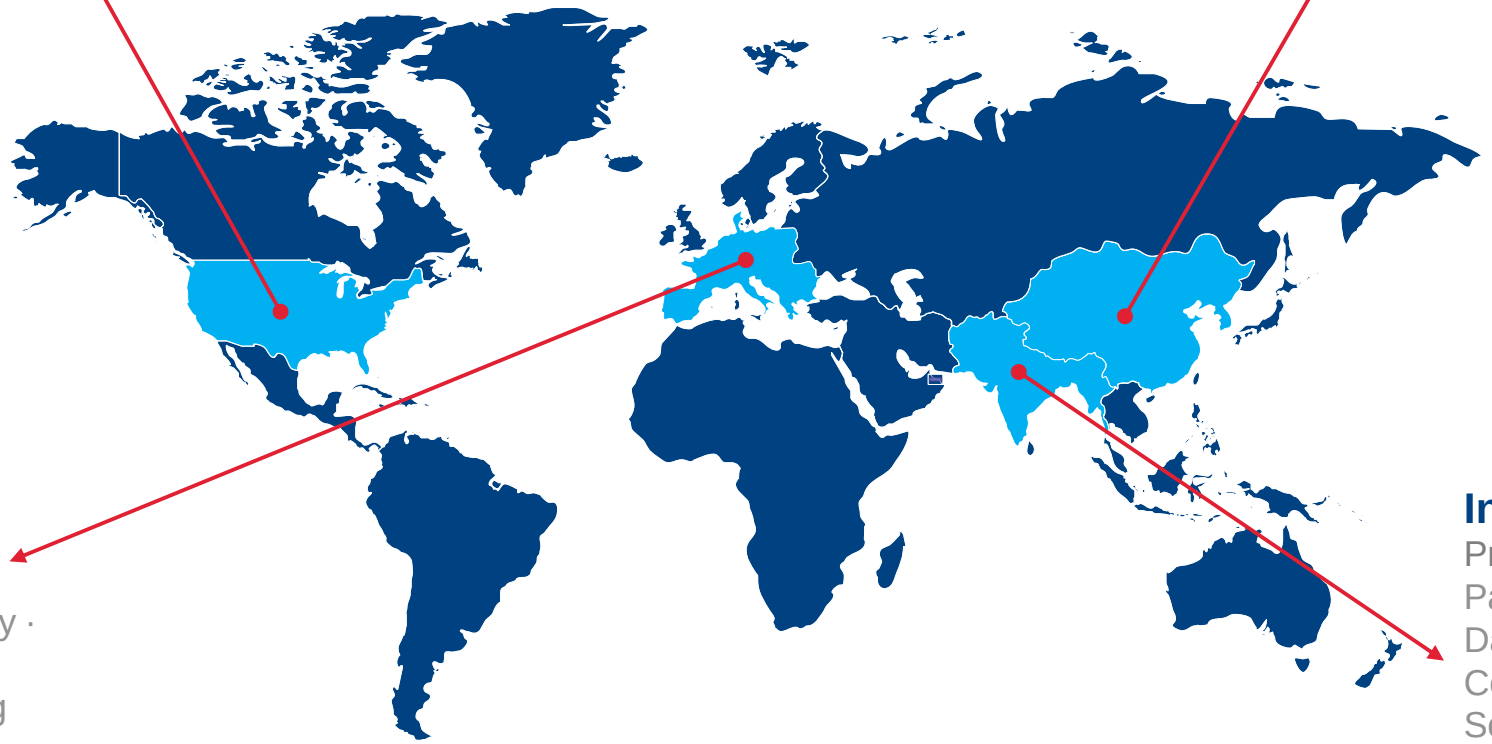
GLOBAL FOOTPRINT

North America

Product Engineering · Data Services · DevOps · Localization · AI Training

Northeast Asia

Product Engineering · Language Services · Agile + DevOps · Retail + Commerce · Data Analytics · Digital QA



Western Europe

Content · Digital Strategy · Mobile Strategy · Localization · AI Training

India

Product Engineering · Payments · Agile + DevOps · Data Integration · Retail + Commerce · Financial Services · Travel · Education · Publishing + Media · Mobility

pactera EDGE

ENGINEERING

- Software + Cognitive Products
- Enterprise + Mobile Applications
- Embedded Technologies
- DevOps
- Product Testing

DIGITALIZATION

- Transformation Consulting
- Digital Products
- Applications + Platforms
- Data + Analytics Modernization

GLOBALIZATION

- AI-Driven Language Services
- AI Enablement Services
- Global Digital Marketing

EMERGING TECHNOLOGIES

- Conversational AI
- Immersive Reality
- IoT
- Intelligent Automation

DIGITAL AGENCY SERVICES (BFM)

USER EXPERIENCE DESIGN

CONTENT MANAGEMENT PLATFORMS

ECOMMERCE PLATFORMS

MARKETING SERVICES

MARKETING ANALYTICS + BI

THE VALUE WE BRING

pactera EDGE

OUR PRODUCTS AND SOLUTIONS LEVERAGE DATA + INTELLIGENGE TO ADD VALUE IN TWO WAYS:

RUN FASTER

Achieve new levels of performance that reduce cost and improve operational efficiency.

RUN DIFFERENT

Add experience-centric digital capabilities to drive greater relevance, revenue + growth.

WORLDWIDE CLIENTS

	NORTH AMERICA & EUROPE	ASIA PACIFIC	CHINA
TECH	vmware, hp, TIBCO, intel, CISCO, Microsoft	lenovo 联想, Alibaba.com, Tencent 腾讯, 南瑞 NARI	SONY, TOSHIBA
BFSI	WELLS FARGO, Prudential, citibank, UBS	中国银行 BANK OF CHINA, 交通银行, 招商银行, 中信银行 CHINA CITIC BANK, 中国建设银行 China Construction Bank, PICC 中国人民保险集团股份有限公司, Bank 中国光大银行 CHINA EVERBRIGHT BANK	BARCLAYS, HSBC, DBS, CommonwealthBank
TELE COMMUNICATION	NOKIA Connecting People, MOTOROLA, Windows Mobile	中国电信 CHINA TELECOM, 中国移动通信 CHINA MOBILE	AAPT, Telecom NEW ZEALAND, TELSTRA, iinet connect better
MANUFACTURING & RETAIL	3M, Abercrombie & Fitch, BOEING, GE, LOWE'S	LG, LI-NING, Haier	DUNLOP, BRITISH AMERICAN TOBACCO AUSTRALIA, pepsi, muRata
OTHERS	Expedia, CONAGRA BRANDS, McDonald's, Ryder, US FOODS	AIR CHINA 中国国际航空公司, 海南航空 HAINAN AIRLINES, 中國東方航空 CHINA EASTERN, CATHAY PACIFIC	Jetstar, AirAsia

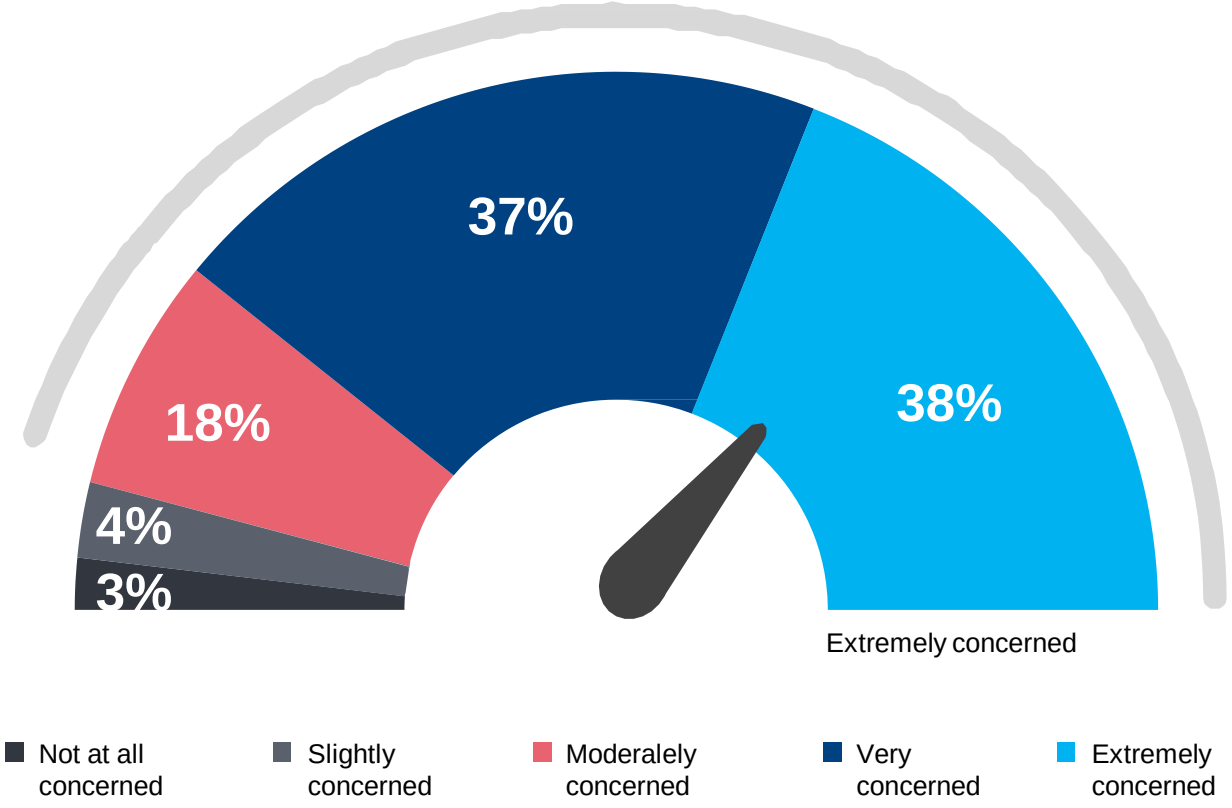
AGENDA

- PACTERA POV AND GARTNER REPORT ON SECURITY
- SECURITY RISK
- A CLOUD SECURITY JOURNEY
- CLOUD SECURITY BENEFITS
- HOW CAN PACTERA SECURITY SERVICES HELP YOU?
- PACTERA MANAGED STRATEGY OF SECURITY SERVICES
- SIMPLIFY SECURITY MANAGEMENT WITH CLOUD
- PACTERA'S SPECIFIC SECURITY SERVICES OFFERINGS
- STRATEGIC SECURITY
- ASPECTS OF CLOUD SECURITY
- SECURE & WELL MANAGED
- DATA ENCRYPTION AND RIGHTS
- SECURITY LIFECYCLE DEVELOPMENT
- SECURITY OFFERINGS FROM OEM'S

PACTERA POV ON SECURITY

- The top cloud security concern of cybersecurity professionals is data loss and leakage (64%).
- Unauthorized access through misuse of employee credentials and improper access controls (42%) takes the number one spot in this year's survey as the single biggest perceived vulnerability to cloud security, tied with insecure interfaces and APIs (42%). This is followed by misconfiguration of the cloud platform (40%).
- The top two operational security headaches SOC teams are struggling with are compliance (34%) and lack of visibility into infrastructure security (33%)

93% Organizations are moderately extremely concerned about cloud security



KEY SURVEY FINDINGS

Cloud security concerns – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year's cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

Biggest threats to cloud security – Misconfiguration of cloud platforms jumped to the number one spot in this year's survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

Cloud security headaches – As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

Legacy security tools limited in the cloud – Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty- four percent say traditional security solutions either don't work at all in cloud environments or have only limited functionality.

Paths to stronger cloud security – For the second year in a row, training and certification of current IT staff (57 percent) ranks as the most popular path to meet evolving security needs. Fifty percent of respondents use their cloud provider's security tools and 35 percent deploy third-party security software to ensure the proper cloud security controls are implemented.

Cloud security budgets increase – Looking ahead, close to half of organizations (49 percent) expect cloud security budgets to go up, with a median budget increase of 28 percent.

SECURITY RISKS

Organizations with defined controls for externally sourced services or access to IT risk-assessment capabilities should still apply these to aspects of cloud services where appropriate.

“When adopting cloud security services, there are four key considerations.

- Where is my data?
- How does it integrate?
- What is my existing strategy?
- What are the new security issues?”

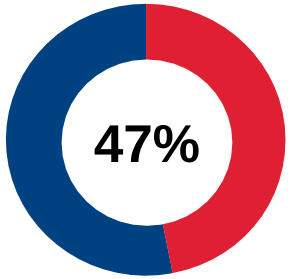
CLOUD SECURITY CHALLENGES

- Identity and access control
- Monitoring and response
- Data leakage
- Governance
- Skills shortages

CLOUD SECURITY CONCERN

67%

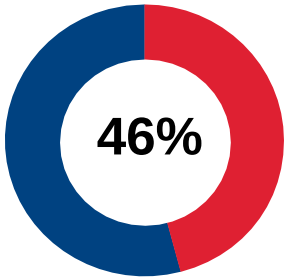
Data loss/leakage



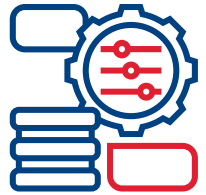
Accidental Exposure

61%

Data Privacy

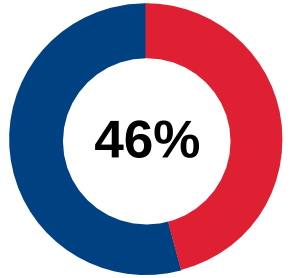


Legal and regulatory compliance



53%

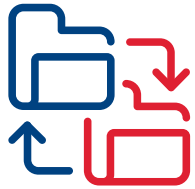
Confidentiality



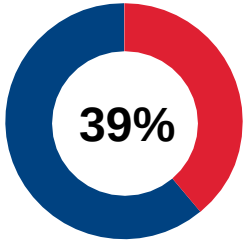
Data sovereignty/ control

Lack of forensic data 37% | Incident response 35% | Visibility & transparency 34% | Fraud (e.g., theft of SSN records) 27% | Liability 25% | Availability of services, systems and data 21% | Business continuity 18% | Disaster recovery 18% | Performance 16% | Other 7%

BIGGEST CLOUD SECURITY THREATS

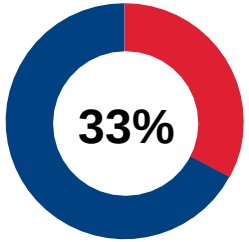


62%

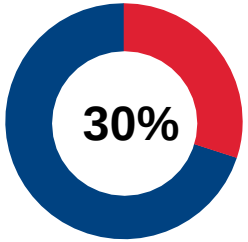


External sharing of data

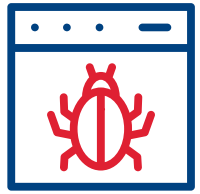
55%



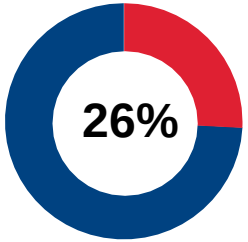
Foreign state sponsored cyberattacks



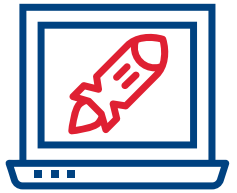
Malicious insiders



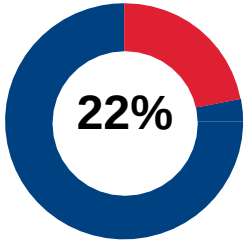
50%



Malware/ ransomware



47%



Denial of service attacks

Theft of service 12% | Lost mobile devices 7% | Not sure/other 7%

A CLOUD SECURITY JOURNEY

Pactera has extensive experience in cybersecurity and threat detection and response. We provide professional services to our customers. The Pactera Services Cybersecurity team is a team of architects, consultants, and engineers that empowers organizations to move to the cloud securely, modernize their IT platforms, and avoid and mitigate breaches.

Services include:

- High value asset protection
- Risk assessments
- Network monitoring
- Threat detection, Prevention and remediation
- Manual and Automated remediations strategies

How we operate

- Our Cloud Security Services are delivered from our global network of ISO27001-certified security operations centers (SOCs).
- Customers are supported by a single team of cloud security experts dedicated to managing their alerts in line with their risk profiles.

CLOUD SECURITY BENIFITS

Happy (compliant) Users

- Secure user self-service
- Increased agility and mobility
- Reduced user frustration
- Less rule-avoidance by users

Segmentation

- Address audit concerns relating to legacy networks
- Improve segregation of duties
- Easier definition of compliance boundaries

Security as a Service

- Best of breed – pay-as- you go/usage-based services
- Mitigate lack of cloud security skills
- Plug & Play security services, e.g. Identity, Endpoint

Automation

- Faster incident detection and response
- Reduction in risk of human error
- Improved resilience and recovery

Target limited resources

- Focus limited security resources on areas that matter most
- Cloud providers deliver physically secure hosting environments – no longer the consumer's problem
- Secure in-house APIs, verify the underlying cloud service

"Shift Left" DevOps & Agile

- Accelerate product delivery
- Assurance of embedded security
- Integrate security within development and operations – DevSecOps

Conclusion

- Your security; your way
- Global scalability and security footprint
- Cost reduction
- Secure digital transformation
- Seamless technology integration
- Digital trust in new services Rapid delivery
- Build secure applications faster.
- Protect every layer of your application.
- Receive guidance to help you succeed.
- Understand and secure your open source software supply chain.
- Integrate security into your open source code-to-code workflows.

HOW CAN PACTERA HELP YOU ON SECURITY SERVICES ?

Assessing and planning cloud security

- Building a complete roadmap for cloud security
- Security strategy and capabilities.
- Identity strategy and alignment
- Information protection and rights management

Threat detection and incident response

- Incident response support (over the phone and onsite).
- Proactive hunt for persistent adversaries in your environment.
- Recovery from cybersecurity attacks

Cloud workload migration and hardening

- Workload analysis, migration, and security hardening
- Hardened consoles for cloud infrastructure administration
- Hardening applications and deployment process
- Designing, implementing, and securing clouds environment.

Administration, identity, and host security

- Hardening administration of cloud services.
- Hardening administration of Active Directory and identity systems
- Hardening infrastructure management tools and systems
- Just-in-time and just enough administrative privileges

Support, operations, and service management: sustaining the gains

- IT support services
- IT staff training
- Health and risk assessments
- Assistance with adoption of recommended practices

PACTERA MANAGED STRATEGY OF SECURITY SERVICES

ASSESS

- Cloud Security Assessment
- Evaluates your existing security environments
- Planned adoption of cloud security

ADVISE

- Cloud Security Advisory
- Decade of helping clients adopt cloud security
- Advise on the design and construction of cloud security architecture
- Mitigate the impact of a massive gap in cloud security

IMPLEMENT

- Enable Cloud Protection Services
- Configuration of identity and access management
- Configure data protection
- Disk Encryption
- Key vault/KMS etc.
- Security group
- MFA/SSO

OPERAE

- Cloud Security Monitoring
- Detects anomalies
- Identified incidents
- IT support services
- Report analytics
- IT staff training
- Health and risk assessments
- Assistance with adoption of recommended practices

SIMPLIFY SECURITY MANAGEMENT WITH CLOUD

Identity & access management

Active Directory

Multi-Factor Authentication

Role Based Access Control/IAM

Azure Active Directory (Identity Protection)

Data protection

Encryption (Disks, Storage, SQL)

Key Vault/KMS

Confidential Computing

Network security

VNET, VPN, NSG

Application Gateway (WAF), Firewall

DDoS Protection Standard

ExpressRoute/Direct Connect

Threat protection

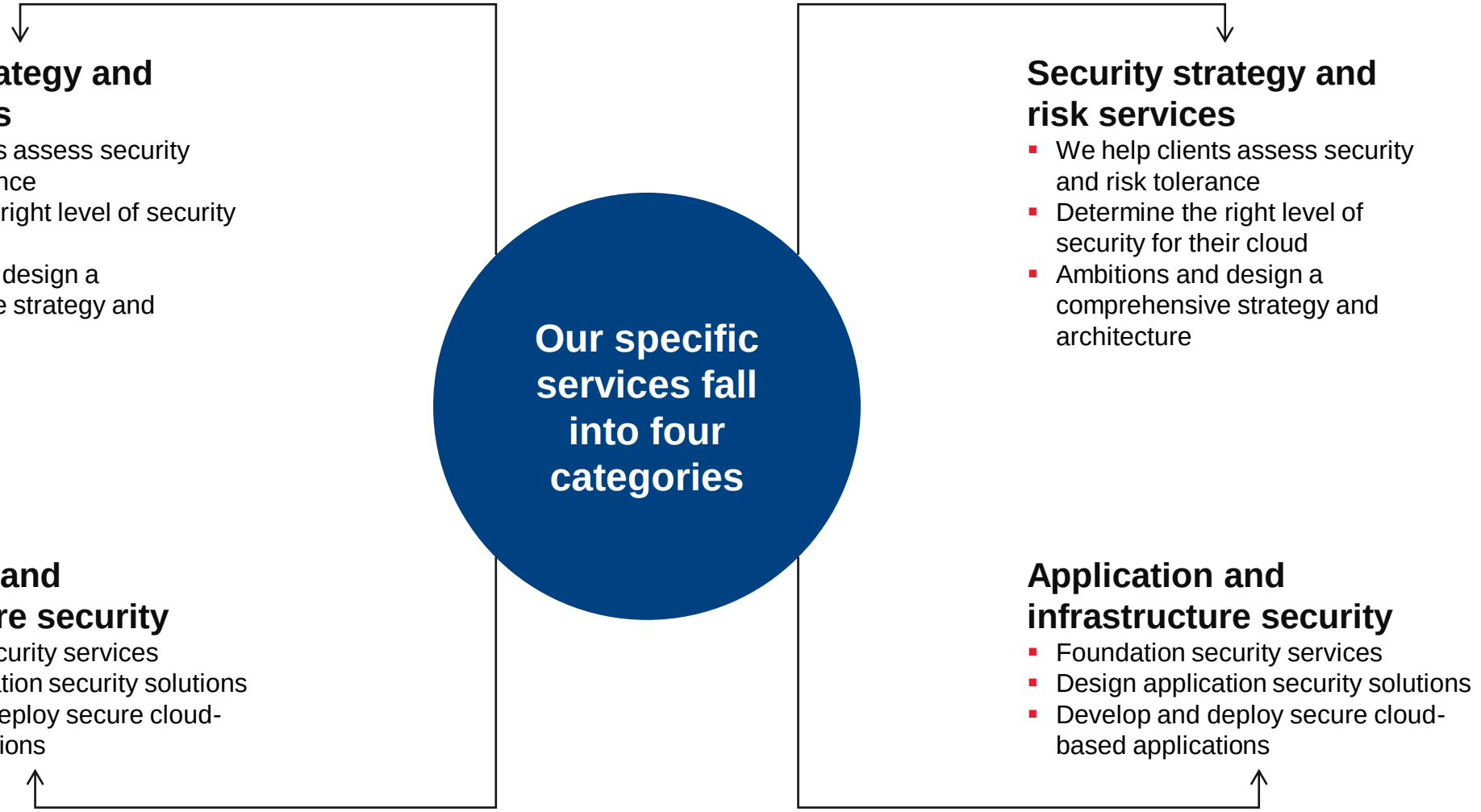
Antimalware

Security management

Log Analytics

Cloud Security Center

PACTERA'S SPECIFIC SECURITY SERVICES OFFERINGS:



STRATEGIC SECURITY

Prevent

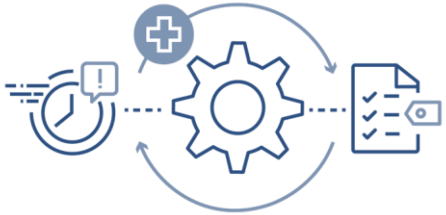
- Define user permissions and identities
- Infrastructure protection
- Data protection

Detect

- Gain visibility
- security posture with logging and monitoring
- Event management, Testing, and Auditing.

Respond

- Automated incident response
- Analyzing root cause



Remediate

- Leverage event driven
- automation to quickly remediate
- secure your AWS environment in near real-time.

ASPECTS OF CLOUD SECURITY

Management Operation Technology

- Updated security policy
- Cloud security strategy
- Cloud security governance
- Cloud security processes
- Security roles & responsibilities
- Cloud security guidelines
- Cloud security assessment
- Service integration
- IT & procurement security requirements
- Cloud security management

Technology

- Access control
- System protection
- Identification
- Authentication
- Cloud security audits
- Identity & key management
- Physical security protection
- Backup, recovery & archive
- Core infrastructure protection
- Network protection

Operation

- Awareness & training
- Incident management
- Configuration management
- Contingency planning
- Maintenance
- Media protection
- Environmental protection
- System integrity
- Information integrity
- Personnel security

TRUSTED CLOUD PRINCIPLES

Security

- Safeguarding
- State-of-the-art technology
- Processes and encryption priority

Privacy & Control

- Privacy design commitment

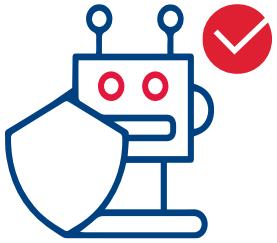
Compliance

- Compliance standards
- Certifications in the industry

Transparency

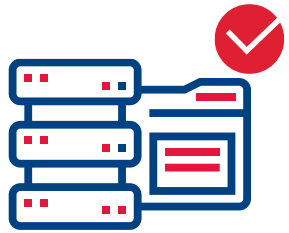
- We explain what we do with your data
- How it is secured and managed

SECURE & WELL MANAGED



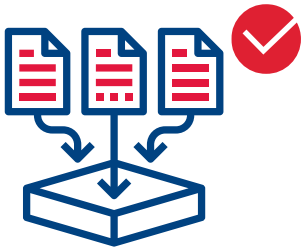
Secure and detect threats

- Install OS patches
- Close firewall ports
- Mitigate threats



Backup your data

- Backup virtual machines
- Select
- Rapidly restore



Get insight using logs

- Monitor CPU, memory & disk
- Troubleshoot applications
- Get insight from logs

For every production instance

DATA ENCRYPTION AND RIGHTS

Data in transit

- Best-in-class encryption
- Secure data

Data at rest

- SaaS services based encryption

Encryption based solutions

- implement additional encryption
- control the encryption method and keys

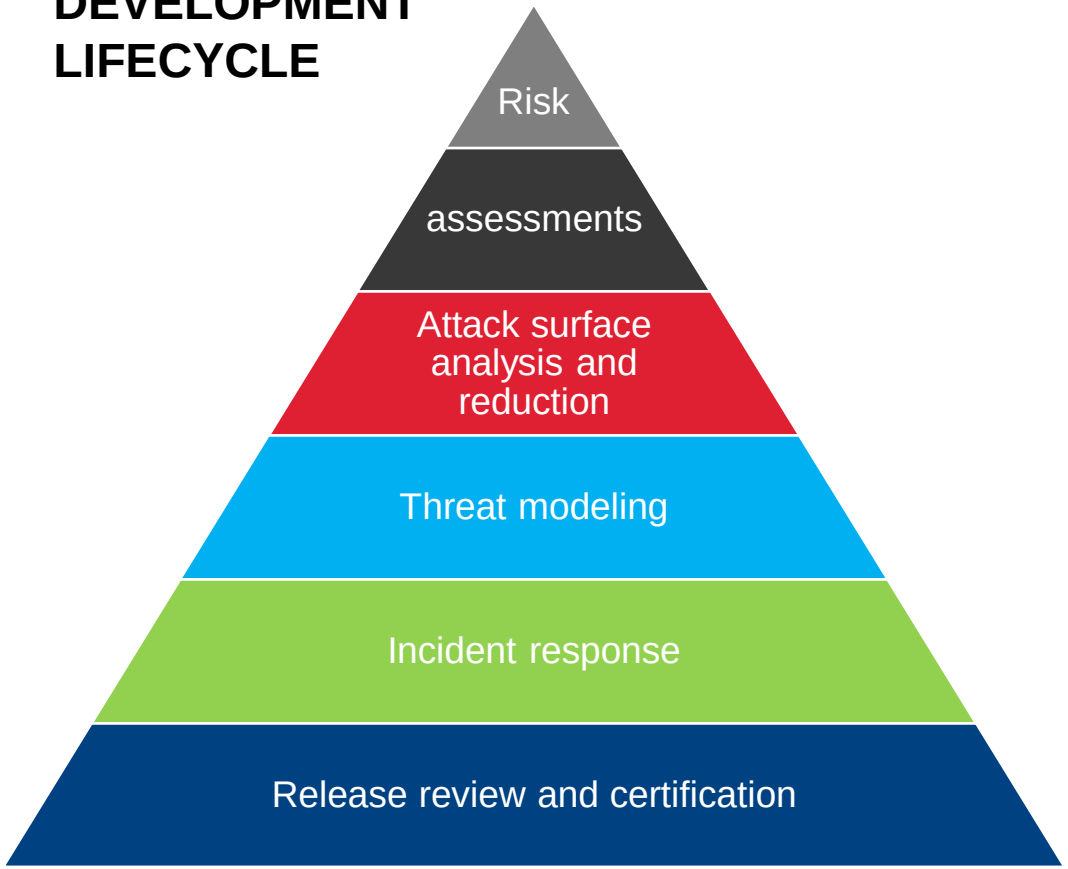
Information Protection

- Encryption,
- Identity
- Authorization policies

Key Vault

- Safeguard cryptographic keys

SECURITY DEVELOPMENT LIFECYCLE



SECURITY OFFERINGS FROM OEM'S

AZURE SECURITY OFFERINGS

Protect your enterprise from advanced threats across hybrid cloud workloads

Azure Sentinel
- Cloud-native SIEM and intelligent security
- Analytics to work to help protect your enterprise

Security Center
- Unify security management
- Enable advanced threat protection

Key Vault
- Safeguard and maintain control of keys and other secrets

Application Gateway
- Build secure
- Scalable
- Highly available web front ends

Azure Information Protection
- Protect sensitive information anytime, anywhere

VPN Gateway
- Establish secure
- Cross premises connectivity

Azure Active Directory & Domain Services
- Synchronize on-premises directories
- Enable Single-sign-on
- Join Azure virtual machines to a domain without domain controller

Azure DDoS Protection
- Azure DDoS Protection
- Distributed Denial of Service (DDoS) attacks

Azure Dedicated HSM
- Manage hardware security modules

AWS SECURITY OFFERINGS

Secure your workloads and applications in the AWS cloud

Data protection
- Protect your data
- Accounts
- Unauthorized access
- Encryption and KMS

Identity & access management
- Securely manage Identity
- Resources and permission

Infrastructure protection
- Protect web application
- Filter traffic
- SQL injection

Threat detection & continuous monitoring
- Continuously thread monitoring

Compliance & data privacy
- Comprehensive view of compliance status

Alibaba Cloud

ALIBABA CLOUD SECURITY OFFERINGS

Anti-DDoS Basic

- Anti-DDoS Pro
- Anti-DDoS Premium

Cloud Firewall

- Web Application Firewall
- Server Guard

SSL Certificates Service

- Cloud Security Scanner
- Managed Security service

Content Moderation

- Anti-Bot Service
- Security Center

GameShield

GCP CLOUD SECURITY OFFERINGS

Google Cloud

Access Transparency
- Visibility over cloud provider
- Near real-time logs.

Binary Authorization
- Deploy trusted Containers on GKS

Cloud Asset Inventory
- View, Monitor & Analyze
- Assets across projects and services by Anthos

Cloud Audit Logs
- Visibility into who did what ?
- User activity logs

Cloud Data Loss Prevention
- Discover and redact sensitive data

Cloud HSM
- Protect cryptographic keys
- Fully managed hardware security module service

Cloud Key Management Service
- Manage encryption keys on GCP

Cloud Security Command Center
- Comprehensive security and data risk platform for GCP.

Cloud Security Scanner
- Automatically scan your App Engine apps.

Shielded VMs
- Hardened virtual machines on GCP.

VPC Service Controls
- Protect sensitive data in GCP services using security perimeters.

Backstory
- Extract signals from your security telemetry to find threats instantly

Cloud IAM
- Fine-grained identity and access management for GCP resources.

Cloud Identity
- Easily manage user identities, devices, and applications from one console.

Resource Manager
- Hierarchically manage resources on GCP

Security key enforcement
- Enforce the use of security keys to help prevent account takeovers.

pactera EDGE