HPE
POINTNEXT

Secure On- and Off-Premises IT Service Delivery Platforms

A Blueprint for Security and Protection in a Hybrid IT World

HPE POINTNEXT BLUEPRINTS: HOW TO GUIDES FROM SERVICES EXPERTS OF HEWLETT PACKARD ENTERPRISE

TABLE OF CONTENTS

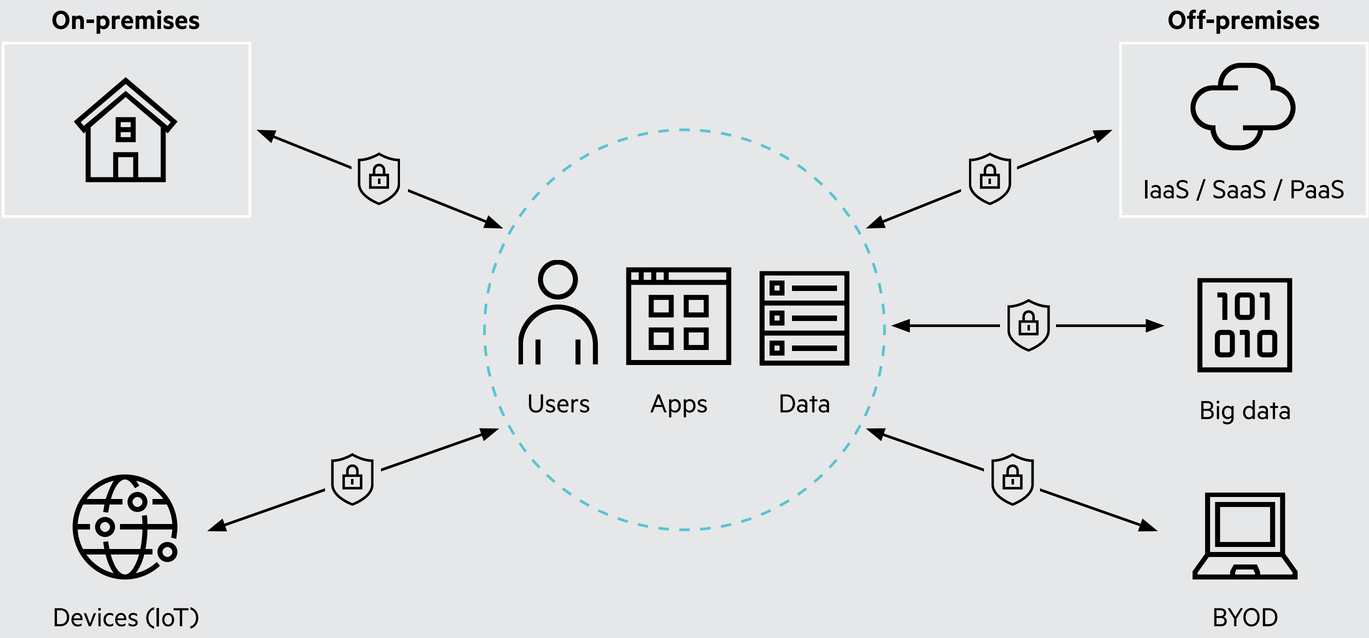
Executive summary

We live in a digital world where everything is changing and where systems, people, places and things are constantly connected.

Competition and changing market dynamics are driving demand for innovation, new experiences and improved efficiencies. But none of this will work without security and digital protection from edge to core to cloud. The overall threat landscape is expanding and constantly changing because mobility, IoT, external cloud services and other digital technologies create new entry points for malware outside the traditional data center. The overall sophistication, funding and orchestration of these attacks is continuously increasing.

This constancy of threat drives the need for constant monitoring across the IT ecosystem to check and remediate any compliance issues. Security is all about risk mitigation. It's critical to be very methodical starting with risk analytics and focus the security measures on the highest, most impactful threats. Security should also be agile and completely pervasive. This requires more automation, innovation, proactive controls, and security technologies that support new platforms across the hybrid landscape that includes the data center, off-premises clouds, mobile devices and the Internet of Things.

Protect your most organizationally critical digital assets and their interactions, regardless of location or device



Challenges

Businesses and organizations are building new hybrid infrastructures to deliver new IT services that require agility, resiliency and security. Success will require more automation, integration and end-to-end visibility supported by threat intelligence and threat analytics. Today, security challenges include:

- Security insufficiently considered when designing service delivery platforms. When designing new IT services, security is often an afterthought or added later. The result is systems that are vulnerable to a wide range of attacks and threats.
- User and system productivity reduced due to complexity of access to applications. Security access systems must be unified and standardized to ensure access control policies are consistently applied with overall improved user experience.
- Security vulnerabilities in applications create significant exposure. Any gap in the security opens access to business data and sensitive personal data that can threaten the life of the organization.
- Cyber threats are becoming more sophisticated making platforms more vulnerable. Security threats have evolved beyond the lone-wolf hacker. Now, criminal organizations and even foreign government sponsored groups are creating increasingly more sophisticated intrusion methods.
- The exponential growth in data creates greater challenges for data security. As data has grown exponentially, so has the threat. More data from more sources creates new intrusion entry points. Privacy concerns also require additional data-centric security.

A Guide to Secure On- and Off-Premises IT Service Delivery Platforms

Most organizations are looking for assistance to address these challenges because they lack the resources and expertise to assess them and respond in a timely manner. HPE Pointnext has developed blueprints that are based on its own digital transformation experience and enhanced through many customer-transformation engagements. These blueprints are customer centric, pragmatic, and aligned to best-in-class tools. They offer a prescriptive-yet flexible, step-by-step process to help guide your journey. This blueprint focuses on securing your on- and off-premises IT service delivery platforms. Each business challenge is addressed through a “Guiding Principle” that includes an overview, a checklist of best practices, and expected results – all focused on security and protection in a digital hybrid world.

Guiding Principle 1: Systematically integrate security across hybrid IT to enable business outcomes.

BUSINESS CHALLENGE: Security insufficiently considered when designing service delivery platforms.

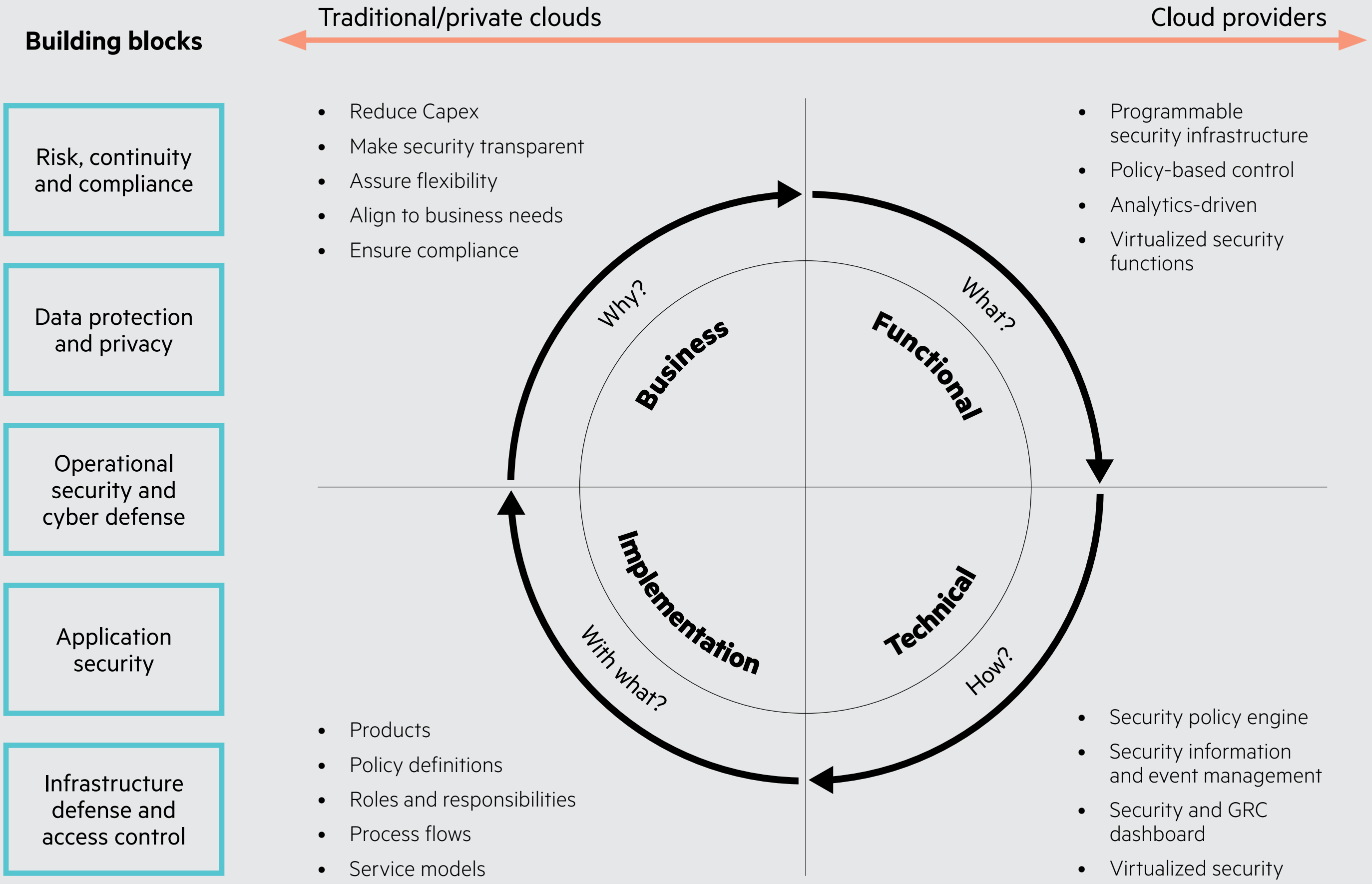
Security cannot be an afterthought or be implemented in an ad-hoc fashion. Security investments should always be driven by specific business needs and risks, defined and then built-in from the start of a project. Security should be implemented in a holistic, consistent fashion and as a continuum across the hybrid IT environments. HPE Pointnext recommends that security be integrated systematically across the entire hybrid environment from planning, to development and deployment. The diagram below shows both the need for an overall framework that will guide the security architecture approach and how it will be applied across the entire hybrid IT environment. Beneath are the security building blocks that will be considered and applied across each phase of the architecture framework.

> 71% of non-IT executives said that concerns over cybersecurity are impeding innovation in their organizations.
>
> **– Source: Cybersecurity at the Speed of Digital Business, Published: 26 May 2016**

Checklist

1. **Stress security-first mindset.** The first step is to change the organization's culture into one that accepts the "security-first" mindset. Security becomes the "anchor" in all infrastructure and application projects.
2. **Assess the organization's risk (business view).** Determine your organization's risk based on threats, your attack surface, and the exposure based on the sensitivity and privacy demands of your data.
3. **Systematically define the right level of security (functional view).** Determine the right level of protection to apply across workloads based on risks and policies. Systematically define the right level of security controls that need to be integrated across hybrid IT to achieve business outcomes, leveraging the Hybrid IT architecture framework.

Hybrid IT protection


Building blocks
Risk, continuity and compliance
Data protection and privacy
Operational security and cyber defense
Application security
Infrastructure defense and access control
Traditional/private clouds
Cloud providers
Reduce Capex
Make security transparent
Assure flexibility
Align to business needs
Ensure compliance
Programmable security infrastructure
Policy-based control
Analytics-driven
Virtualized security functions
Why?
Business
What?
Functional
Implementation
With what?
Technical
How?
Products
Policy definitions
Roles and responsibilities
Process flows
Service models
Security policy engine
Security information and event management
Security and GRC dashboard
Virtualized security

4. **Determine how to apply each building block across your hybrid IT architecture framework (technical view).** The foundation for security starts with five building blocks. Review each area of your hybrid environment and determine how to apply the people, process, and technologies that address them.

   – Risk, continuity, and compliance
   – Data protection and privacy
   – Operational security and cyber defense
   – Application and DevOps security
   – Infrastructure security and access control

5. **Define the specific products and implementation requirements (technical view).** Review your current security portfolio and determine what is required to fill in gaps to protect your organization.

Expected Results

- Reduce the risk and areas of weakness to prevent breaches and data losses by deploying consistent standards and governance.
- Reduce operations costs with integrated security that is consistent and repeatable.
- Provide consistent, end-to-end, and repeatable IT operations aligned to business priorities.

Guiding Principle 2: Make identity the "control plane" for hybrid IT - Align, standardize and simplify identity and access management.

BUSINESS CHALLENGE: User and system productivity reduced due to complexity of access to applications.

Identity must become the new control plane that governs access to hybrid IT resources and services independently of their location. Consistent and seamless identity and access control should be maintained across all on-premises and off-premises environments.

Checklist

1. **Review identity and access management controls.** Identity and Access Management (IAM) is the cornerstone for building secure hybrid IT environments. Review the existing IAM controls and target gaps that must be addressed.
2. **Check for consistent and seamless identity and access control maintained across all environments.** Verify that IAM is consistent across all environments including on-premises and off-premises systems, mobile devices and the connectivity of "things". Integrate the new identity control plane with your enterprise directory services.
3. **Review privileged user accounts.** Pay special attention to the protection of privileged user accounts and the ability to provide detailed activity tracking across the different hybrid IT platforms.

> 59% of senior IT security professionals identified maintaining consistent access security and authorization control across environments as one of their most significant challenges.
>
> **– Source: 451 Research - 2016**

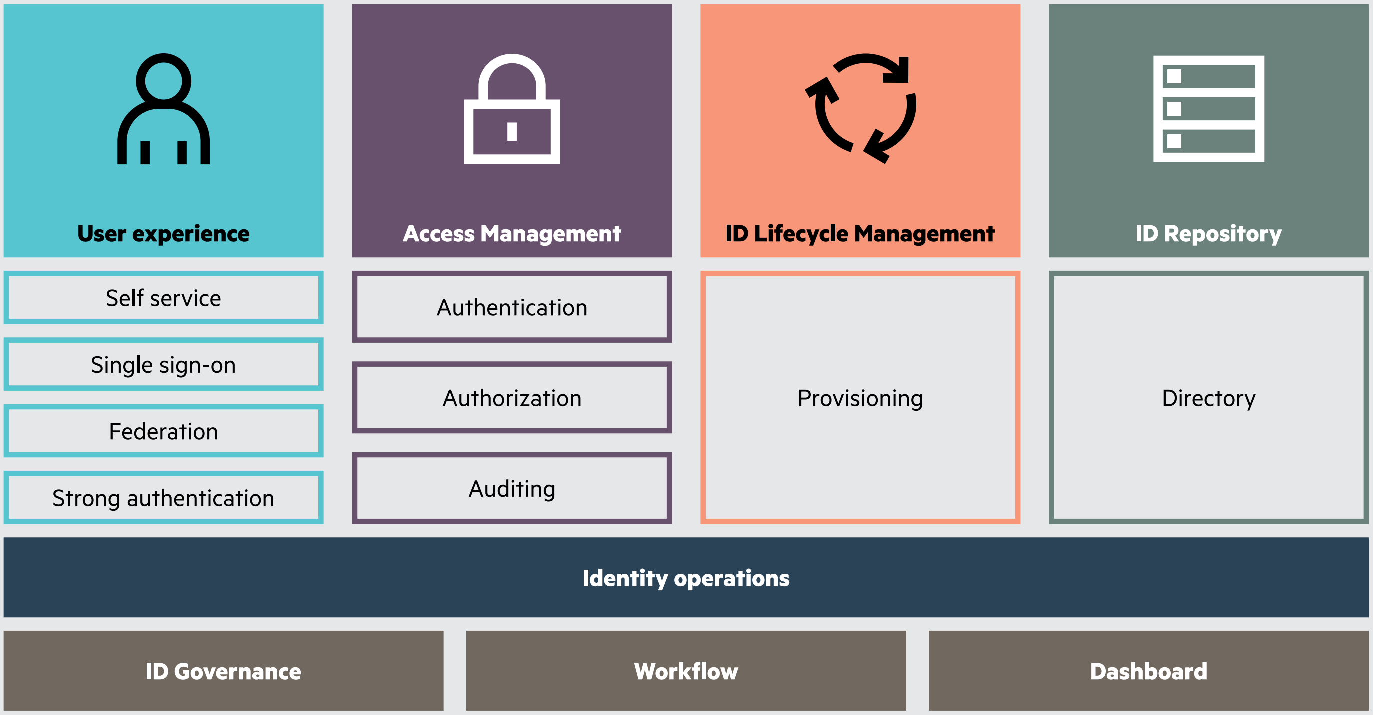
4. **Target identity and access control islands that lack support for open and flexible standards.** Replace with IAM that uses open identity federation standards and solutions.

Expected Results

- Prevent unauthorized access to organizational assets and data while protecting user privacy.
- Control user and administrator access to resources in a fine-grained fashion by federating accounts and access control settings permissions across the different IAM controls.
- Accelerate future enhancements by leveraging the integration of the identity control plane with your enterprise directory services.

Consistent and seamless identity and access control maintained across all environments

Identity the "control plane" for Hybrid IT



User experience

Self service

Single sign-on

Federation

Strong authentication

Access Management

Authentication

Authorization

Auditing

ID Lifecycle Management

Provisioning

ID Repository

Directory

Identity operations

ID Governance

Workflow

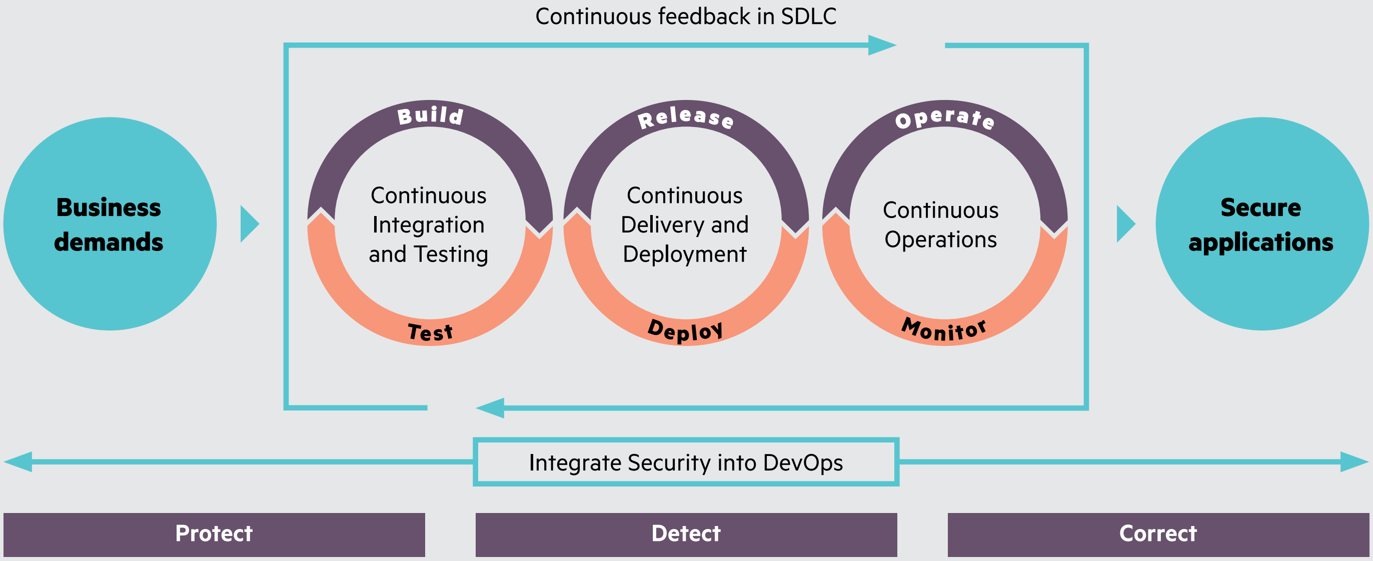
Dashboard

Guiding Principle 3: Utilize DevOps to make security an integral part of development and truly build security practices into the Software Development Life Cycle.

BUSINESS CHALLENGE: Security vulnerabilities in applications create significant exposure.

The always-on requirement of modern IT services, implies that organizations cannot afford any application downtime. Applications that are not secured can cause irrecoverable damage by exposing user and corporate data. They can forever damage the corporate brand and put the organization's very survival at stake. Organizations must improve security and assure universal application protection and availability throughout the application life cycle, and establish an environment that automates continuous monitoring.

Assure Universal Application Protection and Availability



Continuous feedback in SDLC
Business demands
Build
Continuous Integration and Testing
Test
Release
Continuous Delivery and Deployment
Deploy
Operate
Continuous Operations
Monitor
Secure applications
Integrate Security into DevOps
Protect
Detect
Correct

Checklist

1. **Review universal application protection and availability throughout the application lifecycle.** Assess current application lifecycle protection and availability capabilities. Identify gaps in protection. Embed the model into compliance and governance standards.
2. **Build an application protection arsenal.** Update or create a best-fit application lifecycle protection environment that protects, detects potential vulnerabilities, and corrects or recovers from breaches effectively and efficiently. Replace or add new technologies and processes, as necessary, with the goal of integrated protection throughout the entire application lifecycle.
3. **Create a secure DevOps platform.** Design a secure DevOps platform that aligns and optimizes a compliant set of security best practices and tools into integration, testing, delivery, deployment and security operations in the application development lifecycle. Establish a secure continuous delivery platform based on continuous assessment and monitoring.

Expected Results

- Simplify and strengthen application lifecycle security monitoring.
- Enable continuous measurement and remediation of vulnerabilities.
- Assure that the organization's digital assets are unlikely to be compromised through application security weaknesses.

> Organizations are going from four application releases per year in 2010 to a whopping 120 releases per year by 2020.
>
> **– Source: Forrester**

Guiding Principle 4: Orchestrate multiple layers of protection controls for continuous, dynamic and trusted platform security.

BUSINESS CHALLENGE: Cyber threats are becoming more sophisticated making platforms more vulnerable.

Hybrid IT includes a variety of virtual and physical platforms that are either on-premises or in the cloud. One of the compelling advantages of this implementation style is that it allows for the automated migration of workloads between these different platforms and providers. In this dynamic environment, it becomes more critical to assure a homogeneous level of security, availability protection, and resiliency.

Checklist

1. **Build continuous platform lockdown and compliance assessment solutions.** Review existing lockdown and compliance processes and target gaps for improvements and automation. Develop a plan that will cover all aspects of the hybrid IT landscape.
2. **Create integrated layers of protection controls.** Create integrated and defense-in-depth-based layers of security controls including state-of-the-art virtualization and perimeter security technologies.
3. **Implement real-time security and threat analytics engines.** Hybrid IT security requires proactive protection controls that can provide continuous and dynamic platform security assessment and lockdown, and are built on real-time security and threat analytics.
4. **Build agile security operations.** Security should be tightly aligned with IT operations, especially in areas such as patch

> By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.
>
> **– Source: Gartner, 2016**

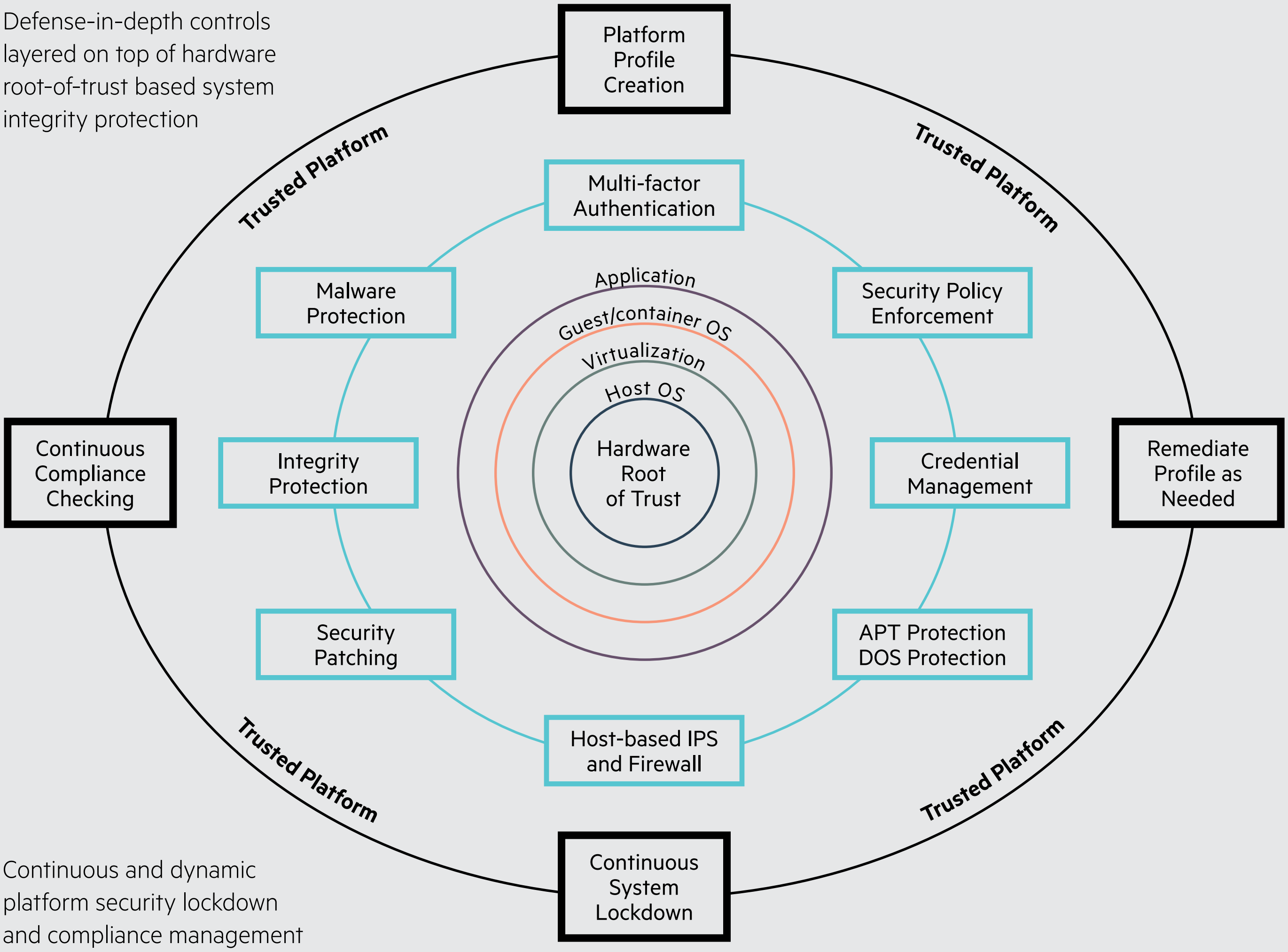
management and platform versions, to be proactive on the latest security vulnerabilities. Security operations must be able to support the ever-changing hybrid IT landscape.

5. **Build hardware root-of-trust based system integrity protection technologies.** Ground your defense-in-depth controls with HPE's root-of-trust based systems for integrity protection starting at the silicon level for integrity protection.

6. **Leverage proactive and behavior-based malware protection controls.** Protect against both insider and outsider malware threats, and intrusions with active monitoring of access control activities.

Expected Results

- Assures platforms are hardened to protect from malware, and both internal and external breaches.
- Improved detection and response to incidents through process automation.
- Confident that business can continue with minimal impact if disrupted by cyber attack disasters.


Defense-in-depth controls layered on top of hardware root-of-trust based system integrity protection
Platform Profile Creation
Trusted Platform
Trusted Platform
Multi-factor Authentication
Malware Protection
Security Policy Enforcement
Application
Guest/container OS
Virtualization
Host OS
Hardware Root of Trust
Continuous Compliance Checking
Integrity Protection
Credential Management
Remediate Profile as Needed
Security Patching
APT Protection DOS Protection
Host-based IPS and Firewall
Trusted Platform
Trusted Platform
Continuous System Lockdown
Continuous and dynamic platform security lockdown and compliance management

Guiding Principle 5: Assure end-to-end data security throughout the entire data lifecycle from creation to destruction.

BUSINESS CHALLENGE: The exponential growth in data creates greater challenges for data security.

Organizations embrace exponential data growth to obtain new business insights. This data comes from a variety of sources outside the organization including mobile, devices, social media and “Things”. The downside is that it creates much more exposure because data travels everywhere in a much larger and more complex attack surface. Legacy security is insufficient, because it cannot guarantee an equal level of protection across locations and throughout the data lifecycle. Traditional platform-centric security should be complemented with a unified data protection approach that attaches security to the data throughout its life.

Checklist

1. Define and implement a modern end-to-end data protection solution. Modern data protection combines data-centric security with end-to-end data protection and builds on solutions that provide “sticky” data protection. Such security and availability controls stick to the data and cannot be circumvented throughout the entire data lifecycle from creation to destruction.

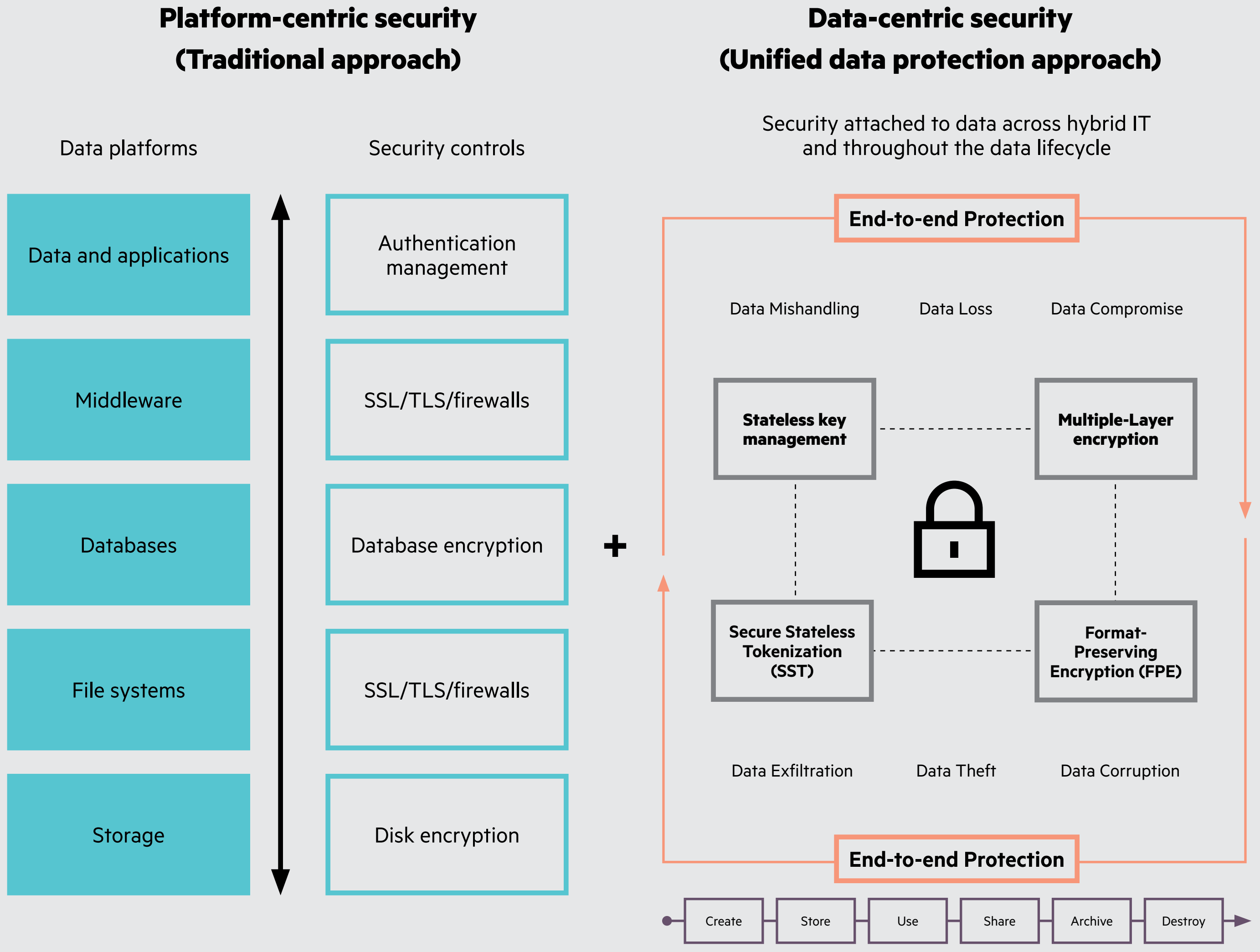
> 55% of senior IT security professionals identified securing the movement of data and workloads across environments as one of their most significant security challenges.
>
> **– Source: 451 Research- 2016**

2. Unify data security across hybrid IT. Adapt new technologies such as stateless key management and tokenization, format preserving encryption, and multi-layer encryption.

3. Leverage HPE Pointnext proven security consulting, design, integration, and implementation expertise. HPE Pointnext designs, implements and integrates solutions from an extensive partner ecosystem of data security and protection technologies.

Expected Results

- Enables the business to bring on new workload models with continuous and adaptive data security.
- Achieve positive scores from internal and regulatory audits and avoid penalties from failed regulatory compliance audits
- Be confident that data is secure and protected no matter where it exists or what stage it is in throughout its journey.



Platform-centric security (Traditional approach)

Data platforms	Security controls
Data and applications	Authentication management
Middleware	SSL/TLS/firewalls
Databases	Database encryption
File systems	SSL/TLS/firewalls
Storage	Disk encryption

+

Data-centric security (Unified data protection approach)

Security attached to data across hybrid IT and throughout the data lifecycle

End-to-end Protection

Data Mishandling

Data Loss

Data Compromise

Stateless key management

Multiple-Layer encryption

Secure Stateless Tokenization (SST)

Format-Preserving Encryption (FPE)

Data Exfiltration

Data Theft

Data Corruption

End-to-end Protection

Create – Store – Use – Share – Archive – Destroy

Case study – Large Government Agency

Business needs

- Develop a government information technology and telecommunications with a view to serve citizens of all ages and provide excellent customer experience.
- Provide greater integration efficiencies across agency subsidiaries through enterprise cloud services.
- Standardize IT infrastructure and significantly lower costs of delivering technology solutions.
- Meet high levels of resiliency and redundancy and as well as stringent government compliance requirements.

HPE solution

- Cloud environment provided IaaS and PaaS to different tenants with complete isolation between them.
- Delivered a custom portal around customer experience.
- Security elements included authentication, virtualization security, encryption, key management, perimeter security and availability technologies.
- HPE Pointnext led the project management, design, implementation and quality assurance on the project.
- HPE Hybrid Cloud Protection Reference Architecture was used to build the entire security framework, including HPE and partner solutions.

Customer outcomes

- Delivered faster, secure and more efficient access to critical IT resources through centralized cloud services.
- Improved ability to drive continuous and open Innovation for government agencies.
- Accepted cloud platform by government agencies.
- Met resiliency and government compliance requirements.

HPE Approach to Protect your Digital Enterprise

HPE Pointnext will work with you from the start of your digital journey to Hybrid IT or to transform elements of your traditional IT security environment. They collaboratively advise, define strategy, develop roadmaps, design architects, integrate and transform so you have adaptive digital protection to compete in the digital economy. HPE Pointnext will help you get from where you are today to where you need to be with highly customizable advisory, transformation and professional services that can help:

- Transform and integrate security to compliantly and reliably enable ubiquitous Hybrid IT consumption models.

- Design and implement security architectures aligned to risks, adaptive to change, and that enable Hybrid IT.

- Optimize and assure security and disaster recovery effectiveness for confidentiality, integrity, and availability through testing and continuous monitoring.

Advisory and Transformation
Envision and define

- Protect Your Digital Enterprise Transformation Workshop
- Hybrid Cloud Protection Workshop, Strategy and Roadmap
- Risk and Business Impact Assessments
- Security Standards and Compliance Assessment
- Operational Security (OpSec) Strategy and Roadmap
- Data Protection & Privacy Strategy and Roadmap

Professional
Design and implement

- Hybrid IT/Cloud Protection Architecture and Design
- OpSec Strategy & Design Service
- Security Monitoring & Incident Management Design
- Security Network Log Management Design
- Platform Protection and Compliance Service

Operational
Consume and optimize

- Foundation Care Services provide support for Gen10 Security features
- Defective Media Retention
- Patch Management Services
- Cyber Resiliency Methodology Training
- Risk Management & BC Planning Training
- Workforce Security Program
- InfoSec Skills & Industry Certifications (CISSP)

Conclusion

Businesses and organizations are under pressure to provide their users with constant innovations to keep up with business demand, be constantly available and highly secure. These requirements translate all the way down to the hybrid IT platforms requiring constant agility, resiliency and security. HPE Pointnext understands and can help with these challenges and demands.

HPE Pointnext will work with you based on where you need the most assistance, whether it be from the start of your journey to Hybrid IT or to transform elements of your traditional IT security environment. They collaboratively advise, define strategy and roadmaps, architect and design, integrate and transform so you have adaptive digital protection to compete in the digital economy. Their methodologies and blueprints are flexible to help with the big picture transformations or with specific solutions to close gaps or improve current security controls, continuity and security operations.

Additional resources

HPE Pointnext

Hybrid Cloud Security for Dummies

Critical Security and Compliance Considerations for Hybrid Cloud Deployments

Hewlett Packard
Enterprise

a00044927enw, May 2018