CITRIX

The secure digital perimeter
for the Citrix Workspace

- **A new security approach**

- **Key benefits**

- **Review the use-cases**

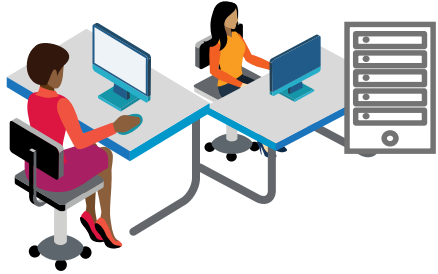**Our Point of View**

SDP story

security

Many point-solutions to protect apps, data, network ...

VDI VCC

App-Ops

NGFW NTA

DLP IPS

SIEM

UEM EMM

MDM

MAM

Adds
IT complexity

UEBA

WAN-OP

SD-WAN

SD-WAN aaS

SSO

VPN

DNS

IAM

CASB SWG

ADC LB

WAF GSLB

Gateway

DDoS SSL

ADCaaS

WAFaaS
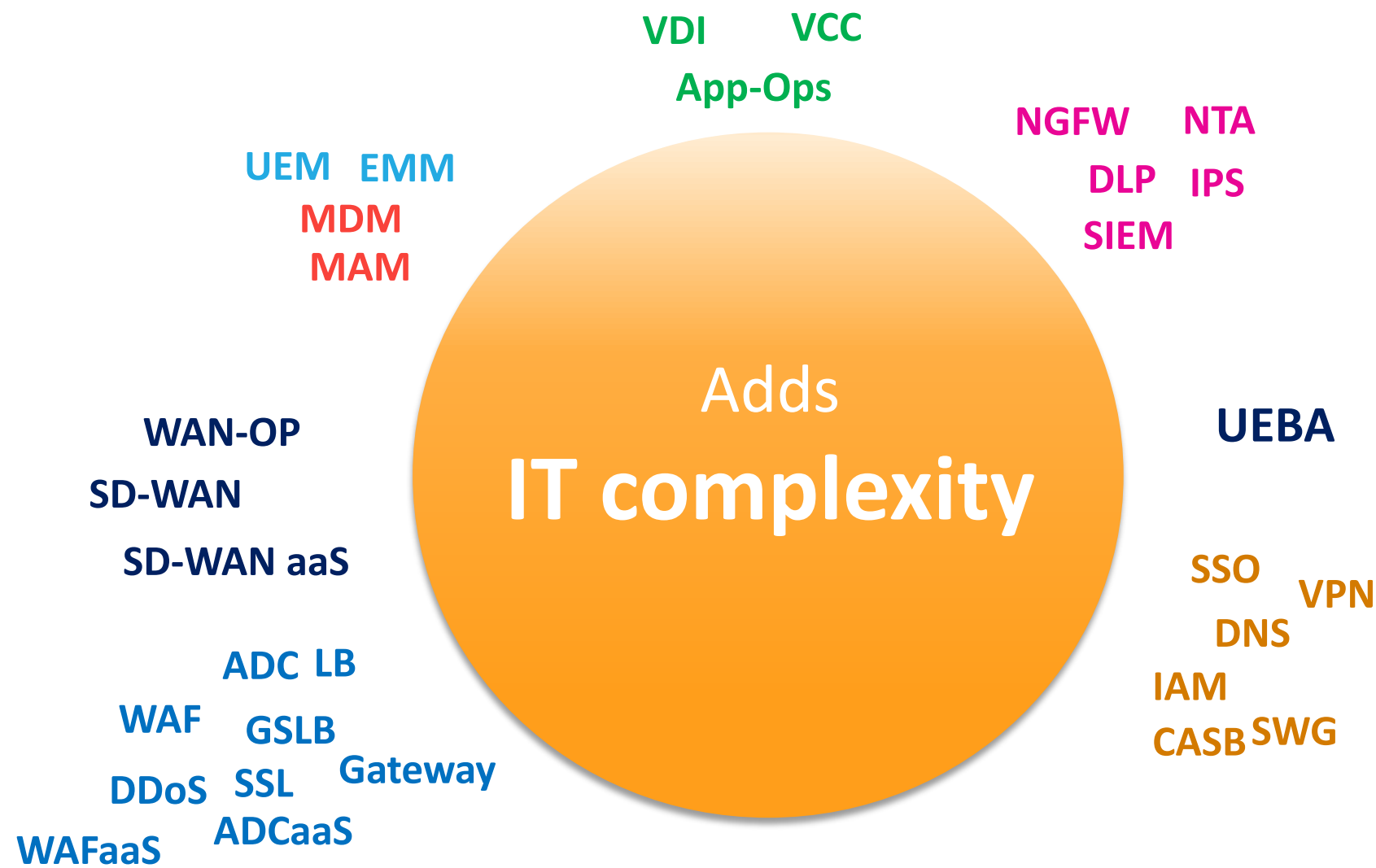
CiTRIX

83% of businesses believe the **complexity** of their organizational structures and IT infrastructure is putting their companies at even greater risk for security breaches.

The Need for a New IT Security Architecture;
Citrix and Ponemon Institute; 2017

CITRIX

Cyber-security is a huge business concern

Attackers with increased motivation driven by monetary value of an attack

88% of execs say they are unable to hire & retain sufficient talent to shore up the security architecture and expertise
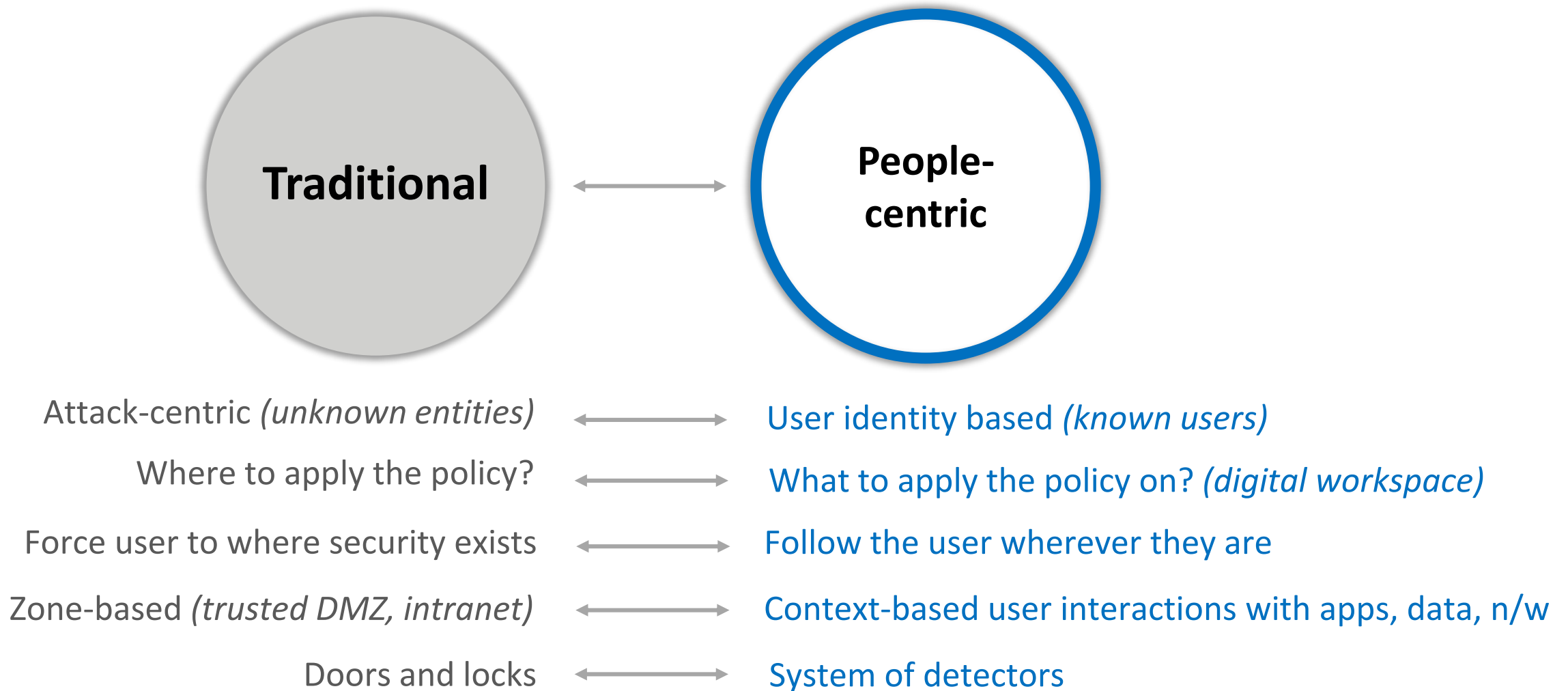
The attack surface is vast and lot more vulnerable for traditional security approaches

CITRIX

Three quarters of enterprises agree the need for a new security framework to address the threat of cyber-security.

- ✓ Cloud & app sprawl
- ✓ Distributed work-styles
- ✓ Un-sanctioned storage
- ✓ BYO and # of devices
- ✓ IT complexity
- ✓ Motivated hackers
- ✓ Vast attack surfaces
- ✓ Malicious behaviors

The Need for a New IT Security Architecture;
Citrix and Ponemon Institute; 2017

CITRIX

A new differentiated approach to security

Traditional ←→ **People-centric**

Traditional		People-centric
Attack-centric *(unknown entities)*	←→	User identity based *(known users)*
Where to apply the policy?	←→	What to apply the policy on? *(digital workspace)*
Force user to where security exists	←→	Follow the user wherever they are
Zone-based *(trusted DMZ, intranet)*	←→	Context-based user interactions with apps, data, n/w
Doors and locks	←→	System of detectors

CiTRiX

Security for the digital workspace

Secure Digital Perimeter

Evolve from *attack-centric* to **dynamic** *people-centric* perimeter security

Unified Endpoint Mgmt.

App Ops

Content Control

IT/Networking

...urity & Performance Analytics

CITRIX

Why is SDP important?

With application sprawl, **the network** is critical to securely delivering apps, content and workspaces.

The SDP approach **significantly expands Citrix Networking offerings** in a SaaS, hybrid, multi-cloud and multi-device world

... enabling **simplified control**, **360⁰ visibility** and **intelligent analytics**

SDP – Trusted security for the Citrix Workspace

Simplified **control**

- On-demand *people-centric*

- Centralized policy control with distributed enforcement

- Minimize/hide attack surfaces

- Easier IT & regulatory compliance

360 **visibility**

- Aggregate logs and transaction flows

- Full visibility across SaaS, hybrid and multi-cloud

Intelligent **analytics**

- Share threat intelligence across services

- Detect and stop malicious user-behaviors

- Trigger contextual actions & policies

CITRIX

Benefits

security

Citrix SDP provides …

1. Contextual and **secure access**

2. Mobile and **device security**

3. User security and **malware protection**

4. Secure collaboration with **content security** and intellectual property (IP) protection

5. Governance, risk and **compliance**

6. Business **continuity** and app security

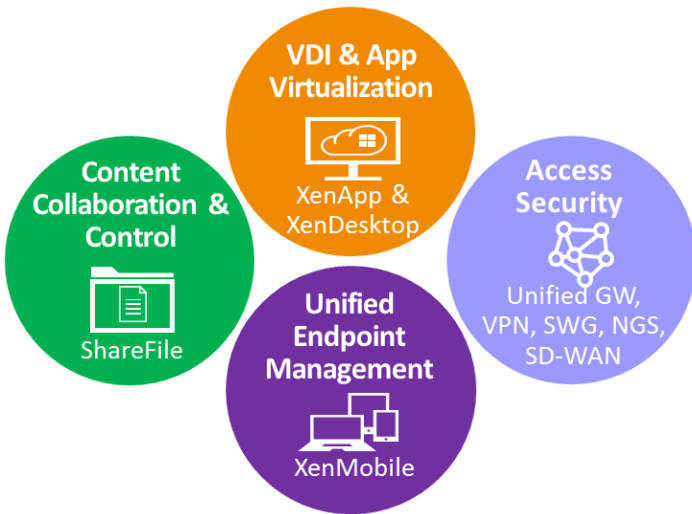7. User **behavior analytics** and proactive security insights

Use Cases

security

Contextual and Secure Access

*The Citrix Identity and Access Management/IDaaS solution provides single sign-on and secure access to the secure digital workspace.

**Citrix solutions provide end-to-end security to apps deployed in datacenter, cloud, or SaaS to user accessing from branches, hospital clinics, or remote sites while using any device.

Use Cases

*Implement identity and access management (IAM) solution in federation with AD and AzureAD (AAD)

**Branch, campus and remote users access applications in datacenter, public Internet or cloud ... securely, from any device
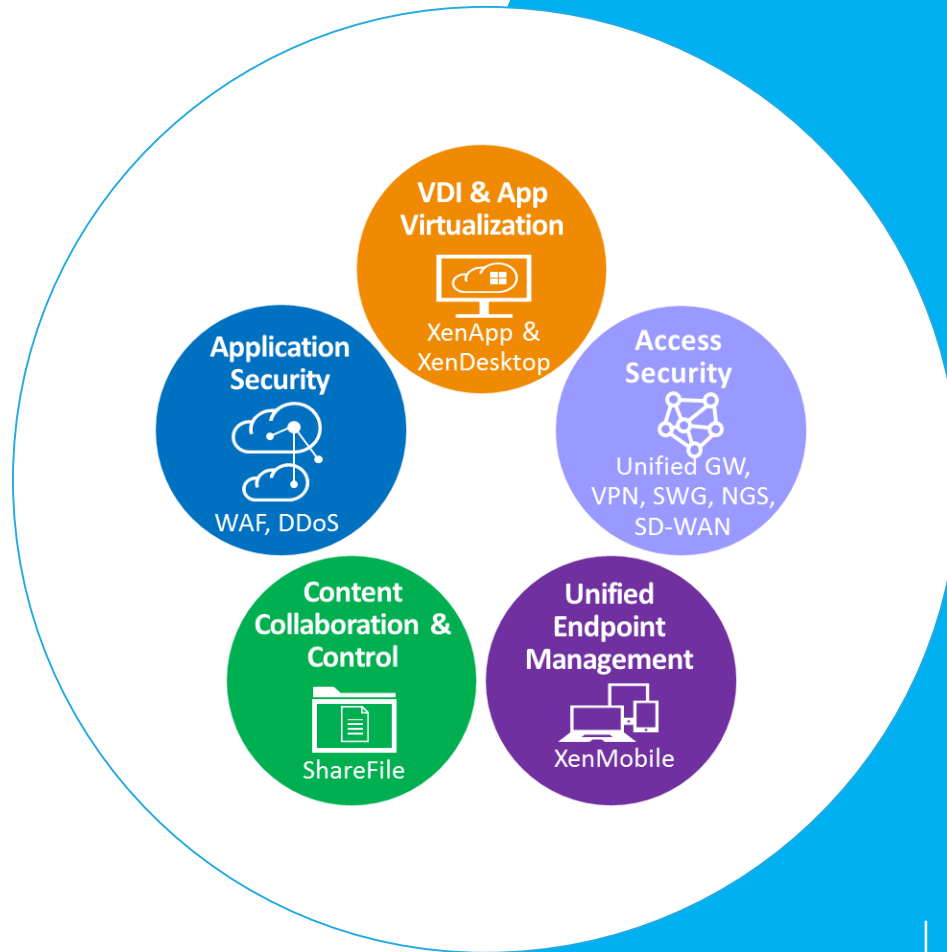
CITRIX

Mobile and Device Security
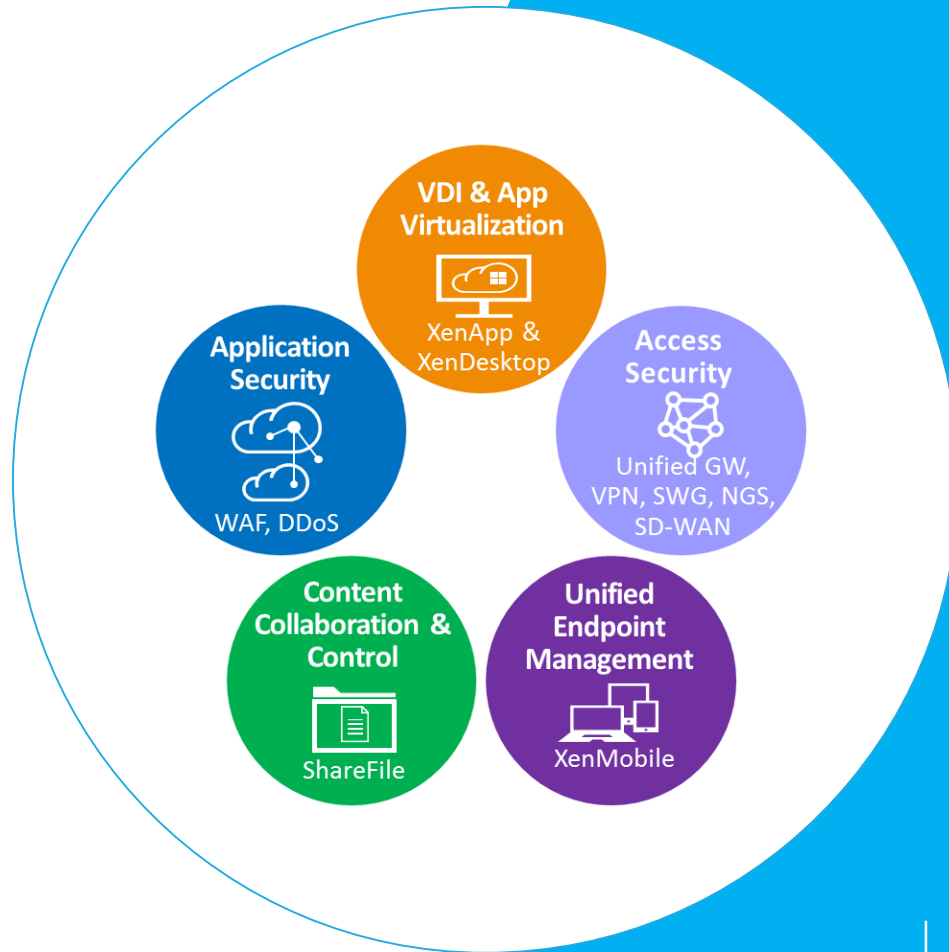
Citrix improves user productivity by delivering secure access to corporate apps from both personally owned and corporate issued devices.

Use Case | **Customers looking to implement BYOD and protect application data on mobile devices**

CITRIX

User security and malware protection

VDI & App Virtualization
XenApp & XenDesktop

Application Security
WAF, DDoS

Access Security
Unified GW, VPN, SWG, NGS, SD-WAN

Content Collaboration & Control
ShareFile

**Unified Endpoint Management**
XenMobile

The secure digital perimeter (SDP) framework provides a differentiated and coordinated approach to protecting against malware and ransomware given the multiple touch points we can detect – endpoint (XenMobile), network path (Secure Web Gateway), content repositories (ShareFile), and applications (XenApp and XenDesktop).

Use Case

Secure the end-points and application infrastructure from malware threats and ransomware attacks
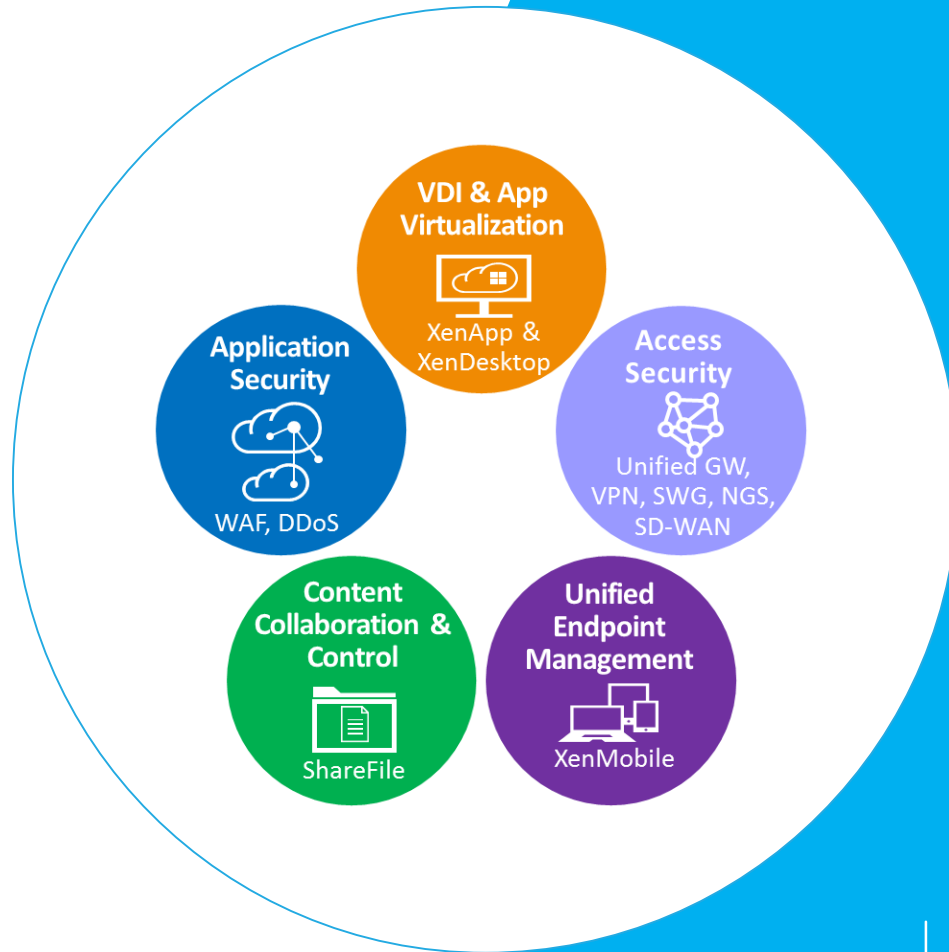
CITRIX

Secure Collaboration
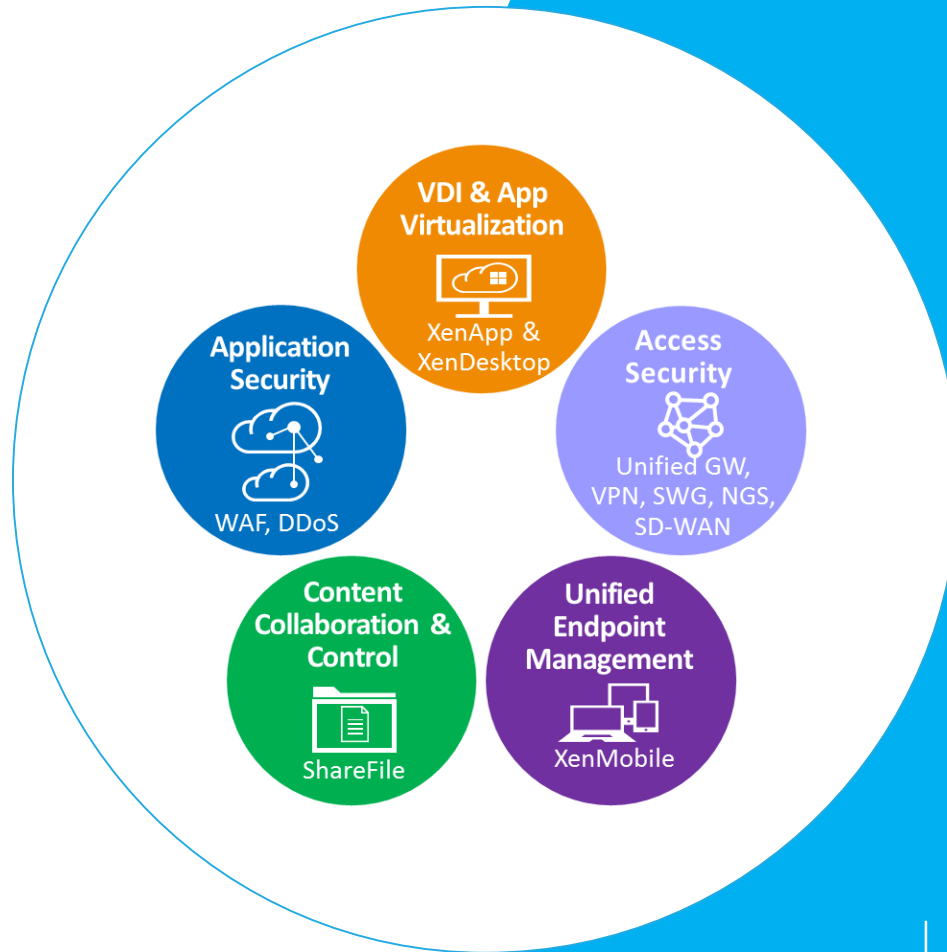
With Citrix ShareFile, the secure digital perimeter (SDP) framework offers a comprehensive solution across users and apps that supports easy access and collaboration while protecting data against theft, misuse and loss.

Use Cases

- Protect confidential information and intellectual property
- Secure collaboration and file sharing
- Use Information Rights Management (IRM)

CITRIX

Governance, risk and compliance

VDI & App Virtualization
XenApp & XenDesktop

Application Security
WAF, DDoS

Access Security
Unified GW, VPN, SWG, NGS, SD-WAN

Content Collaboration & Control
ShareFile

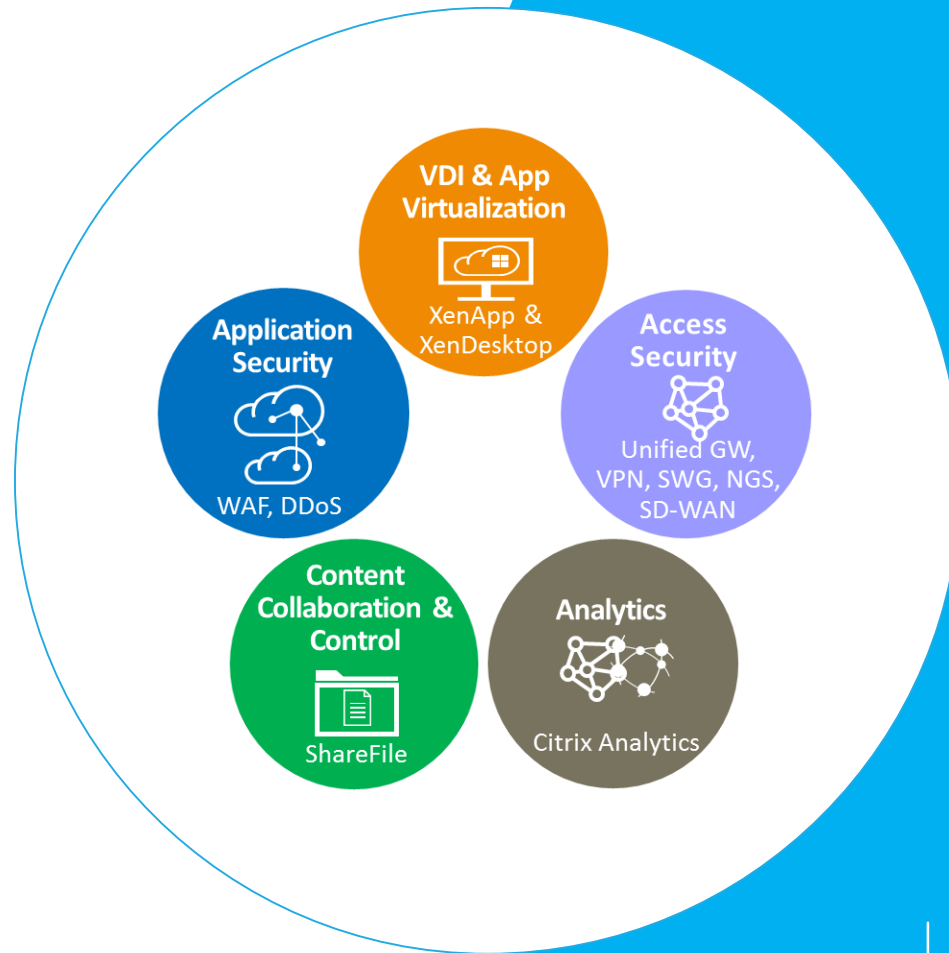**Unified Endpoint Management**
XenMobile

Citrix helps customers address risk, global compliance standards, and industry regulations for app, user and device security using the secure digital perimeter (SDP) framework.

Use Cases | Reduce business risks by implementing compliance standards, adopting industry regulations and adhering to internal policy governance.

CITRIX

Business Continuity and App Security

VDI & App Virtualization — XenApp & XenDesktop

Application Security — WAF, DDoS

Access Security — Unified GW, VPN, SWG, NGS, SD-WAN

Content Collaboration & Control — ShareFile
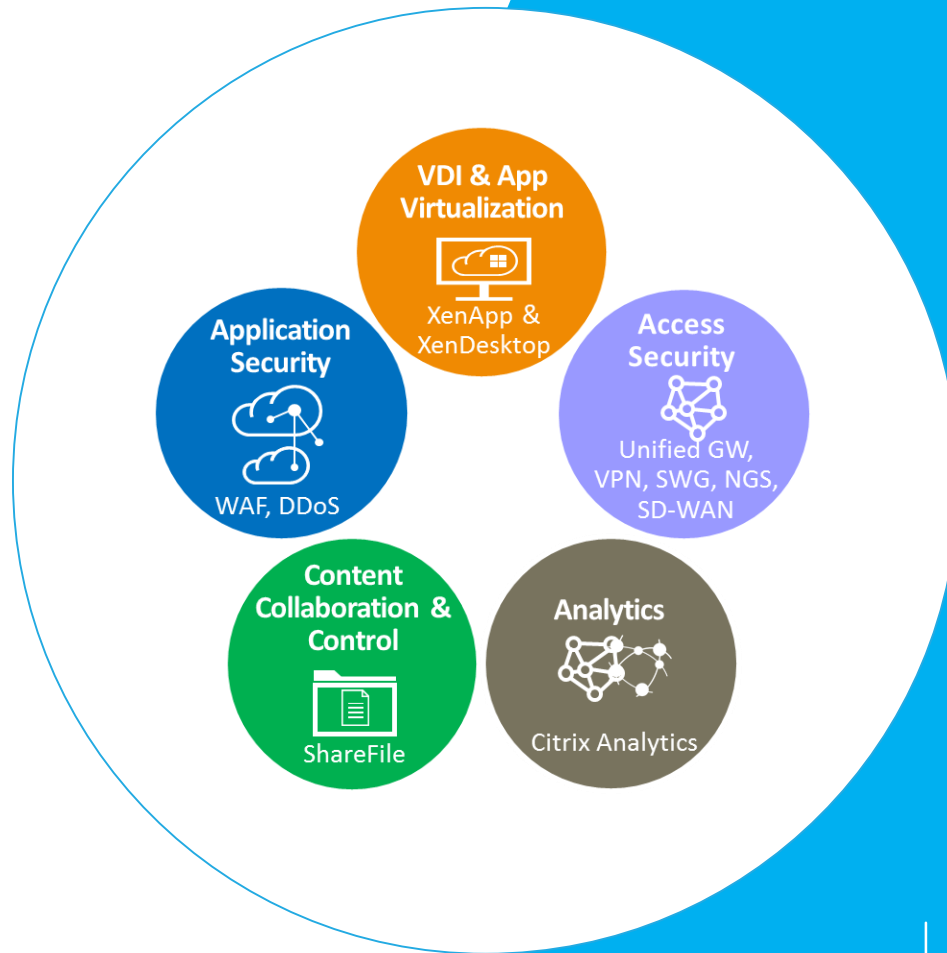
Analytics — Citrix Analytics

Using the secure digital perimeter (SDP) framework, Citrix provides business continuity by 1) preventing malicious attacks from affecting business operations and 2) providing network and secure access resilience during outages, natural disasters and calamities. This enables the workforce to rapidly resume essential and critical activities industries such as law enforcement, healthcare, and finance.

Use Cases

- **High Availability and better performance of web and virtual applications.**
- **Implement a defense-in-depth (availability and security) for applications in the datacenter and cloud, and actively monitor the application infrastructure for external or internal attacks.**

Citrix

User behavior analytics and proactive security insights

As a key component of a secure digital perimeter (SDP), Citrix Analytics collects data across Citrix offerings, generating actionable insights that enable administrators to proactively handle user and app security threats, improve performance and support continuous operations.

Use Cases

- **Protect users and endpoints from external and internal threats.**
- **Protecting enterprise from internal rogue and compromised users.**
- **Secure application infrastructure from external and internal threats.**

CiTRIX

Simplified Control

360 Visibility

Intelligent Analytics

Trusted security for the 'secure digital workspace'

- New dynamic people-centric approach to security in a SaaS, hybrid, multi-cloud and multi-device world

- Centralized policy engine with distributed enforcement

- Integrate with all Citrix products – protect existing investments

- Full visibility and security analytics to mitigate risk

- Protect app infrastructure and minimize/hide attack surfaces