



Applications and data are everywhere.  
How protected are you?



[www.cybertek.net](http://www.cybertek.net)





In a modern business environment, people interface with applications more often than with people, and performance expectations are high.

People are more reliant on applications and digital services to increase productivity and manage their businesses.

Applications are the foundation of businesses:

**46%** of organizations feel that half their revenue will be influenced by digital in 2020.

Source: ZDNet

The value of digital transformation for both society and industry could reach **\$100 trillion** by 2025.

Source: World Economic Forum



The evolving application landscape creates complexity, and data is being created everywhere.

A simple and intuitive experience often hides a complex architecture that enables an application's experience.



#### Applications are evolving

- Refactoring and cloud-native need modern architectures and capabilities
- ML, AI, and analytics place new demands



#### Developers demand multicloud flexibility

- Unprecedented application development speed and scale
- IT complexity driven by inconsistent buying options



#### Workloads are more distributed

- Require flexible placement, increased performance, and enhanced monitoring
- Increased attack surfaces and blind spots

By 2020, more than **40%** of data science tasks will be automated.

Source: Gartner

**93%** of cloud adopters intend to be using multiple clouds in the next 12 months, and **58%** work with at least four vendors.

Source: IDC



Cyber criminals are exploiting undefended gaps in security.

Traditional cyber threat protection strategies are out of step with the expanding perimeter and evolving threat landscape.

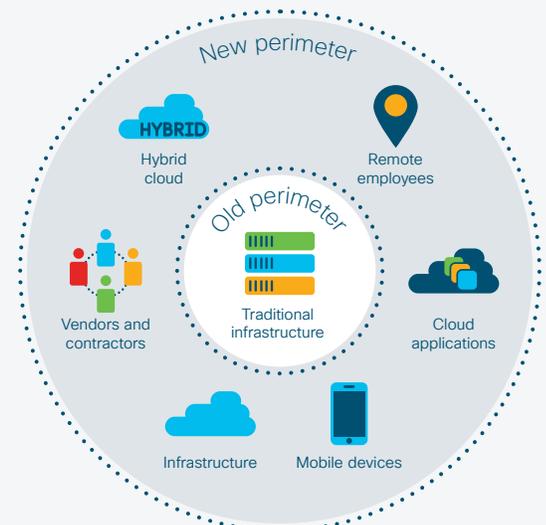
Security teams are spending **76%** of their time defending the data center—the old perimeter.

Meanwhile, **81%** of breaches are via weak or stolen passwords. **86%** of malware is via web or email. Attackers are targeting the weakest links: the users and applications—the new perimeter.

Source: 2017 Data Breach Investigations Report (DBIR), Verizon

It takes an average of **191 days** for businesses to detect a security breach.

Source: The 30 Cybersecurity Stats That Matter Most, TechBeacon, 2018





This changing application landscape demands a more agile infrastructure.

Build on the secure data center using building blocks that help ensure infrastructure agility through automation of policies and comprehensive security.



### Infrastructure

Build a system designed to optimize workloads, regardless of form factor or location.



### Automation

Automate wherever possible to transform IT into an agile and strategic business enabler.



### Security

Integrate security from the ground up, providing pervasive visibility and defense.



By 2022, 40% of operational processes will be self-healing and self-learning.

Source: *Operating Model Transformation Leverages Connected Systems*, IDC, 2018



The changing threat and infrastructure landscape requires a new approach to security...

...that helps ensure the visibility of applications and data, restricts unnecessary privileges and access, and enables rapid threat detection and remediation.



### Visibility

“See everything”

Gain visibility into all users, workloads, and applications in a data center. A data center is a “black hole” without this visibility, and we can’t protect what we can’t see.



### Segmentation

“Reduce the attack surface”

We use this information to develop a policy to segment the data center. This keeps “bad actors” from accessing the whole data center if they are successful in breaching the perimeter.



### Threat protection

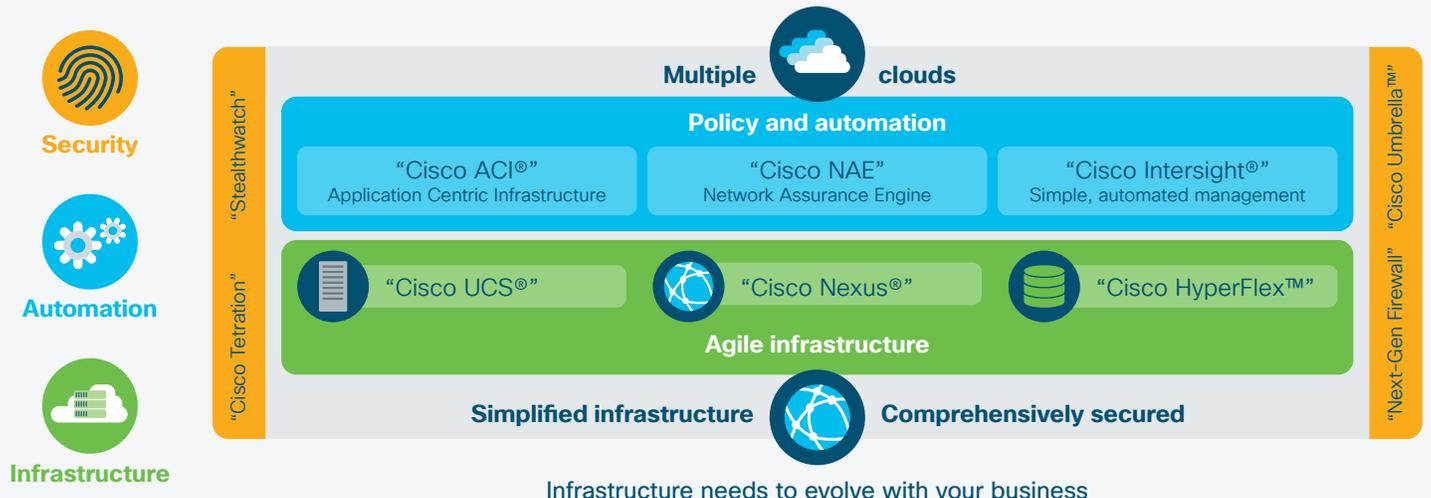
“Stop the breach”

We deploy security products that quickly detect breaches and then work with the data center infrastructure to rapidly remediate.



Only Cisco and our Ecosystem can deliver an agile yet secure infrastructure for today’s digital business...

...with a proven validated design that works together seamlessly, reducing operational overhead while providing agility to provision applications quickly and securely, regardless of data center location—public, private, or both (hybrid).



## Customer voice

“ Cisco ACI allowed us to stretch the network fabric seamlessly across both data centers. And it was the only solution that gave us single-pane-of-glass management.”

Director of IT, ProMedica

“ We wanted to standardize our network architecture and IT operations worldwide using policy-based automation so that changes could be made universally.... With Cisco ACI, we can develop standardized scripts and policies and then push them to all of our sites.”

Senior Network Engineer, Experian

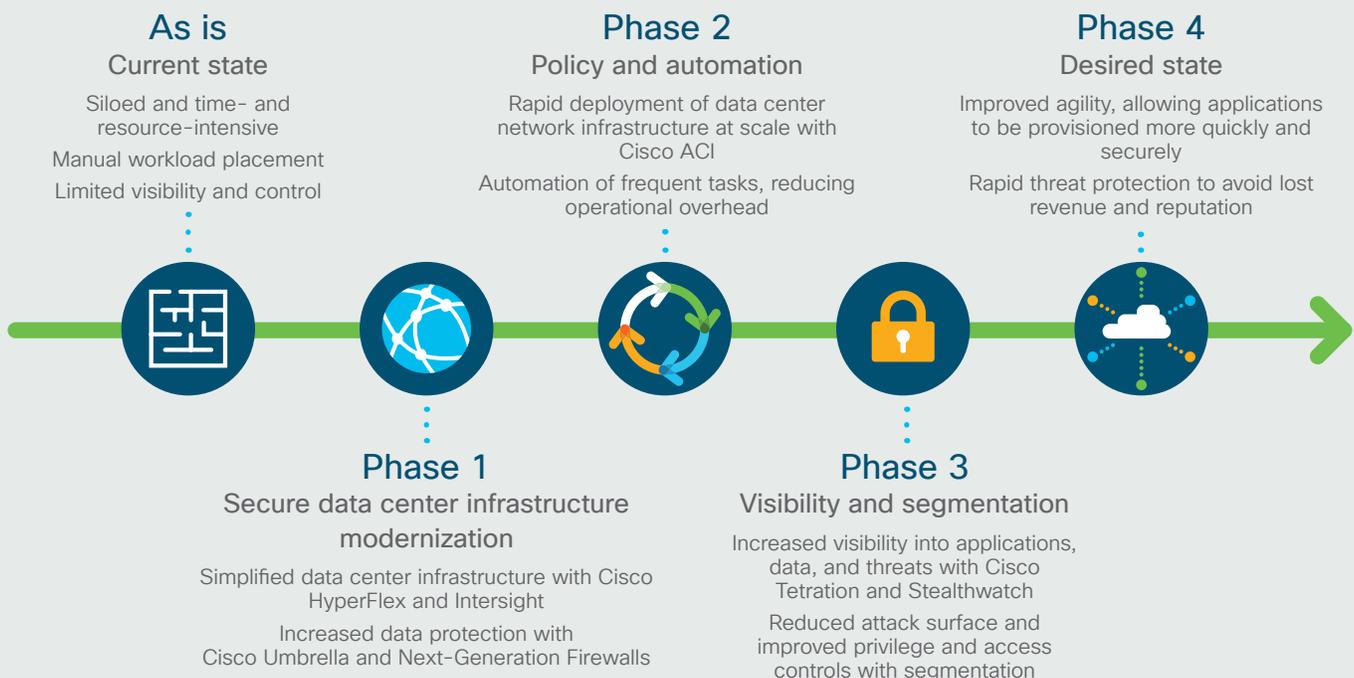
“ We first deployed Tetration, then ACI, and will deploy NAE. That will give us security, visibility, and availability. We will soon be in a position where the data center will never be down again.”

CIO, FNB

## Next step

Book a workshop with Cisco data center and security experts to help get you started on your secure data center journey.

### The journey to an agile, secure infrastructure for today's digital business



Your time is valuable, and system downtime can erode your productivity. At Cybertek, we pride ourselves on being able to work with any schedule in order to minimize your downtime. Whether it's internet security or wireless networking, our team of experts



[www.cybertek.net](http://www.cybertek.net)

