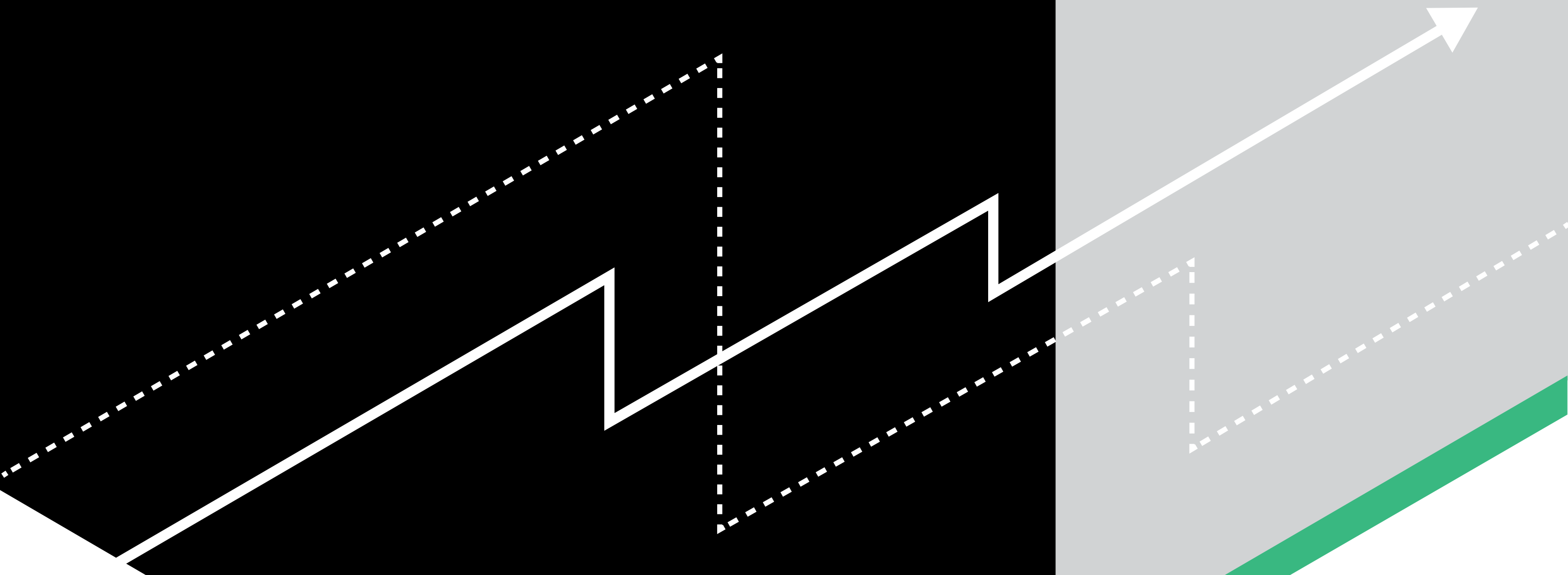
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

October 2020

How To Get From Here To Zero Trust



FORRESTER®

Table Of Contents

Project Director:
Lisa Smith,
Principal Market Impact Consultant

Contributing Research:
Forrester's Security & Risk
research group

Executive Summary

The global COVID-19 pandemic has exposed gaps in the security infrastructure for enterprises around the world. As countries and companies worked to mitigate the impact to people and business operations, a host of issues has risen to the surface. At the outset of the coronavirus pandemic, business operations needed to transform almost overnight, as a large percentage of workers began working from home. This shift increased a reliance on not only mobile devices, but also on a distributed infrastructure environment. Over time, businesses also increased their adoption of services and applications in the cloud. The speed and complexity of this transformation exposed some organizations to new security risks.

The initial rush towards remote work now shifts to a sustained effort as we enter the later stages of the pandemic, and organizations are focusing on going back and securing their distributed employees, devices, enterprise applications, and cloud environments using a combination of security and IT management. Security leadership wants to find ways to reduce environmental complexity and increase their team's efficiency and precision.

VMware commissioned Forrester Consulting to consider how organizations are securing distributed environments with intrinsic security capabilities, and Zero Trust strategies. Identifying key technological and policy milestones associated with the most successful implementations will help others move forward on their journey toward Zero Trust.

KEY FINDINGS

› **The explosion of data, applications, remote users, mobile devices, and bring-your-own-device (BYOD) capabilities has increased security risks.** This explosion has increased the potential blind spots for security teams trying to identify and control enterprise risks.

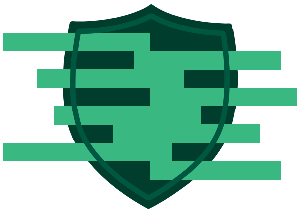
› **Enterprises are vulnerable, as distributed environments can shade visibility and increase attack area.** More than 75% of respondents report an increased level of vulnerability in their organizations due to an increased attack surface. Additionally, too many disparate security solution and integration challenges leave gaps in security protection.

› **Technology solutions can make or break your security strategy.** Our research found that 70% of enterprises lack a cohesive security strategy. And while IT leaders are facing more pressure from the board, they are also grappling with cultural issues between IT and security teams.

› **Zero Trust is the relief to these challenges.** Forrester's Zero Trust strategies can provide a roadmap for enterprises to follow in order to overcome these challenges and mitigate security risk.

› **Intrinsic security reduces complexity and costs.** Intrinsic security solutions are built-in versus being bolted-on, and they have the opportunity to increase collaboration with IT, operations, and security teams. This allows faster investigation and remediation and reduced complexity, which ultimately leads to reduced capex and opex.

The Varying Security Dynamic Increases Risks



Prior to the pandemic, business models required enterprises to actively transform how they utilize business technology to win customers and enable their workforce. In the current environment, adopting Zero Trust security strategies are more important than ever. And to successfully secure distributed environments, companies must take a data centric approach to security because:

- **The growth in remote users, BYOD, and device platforms further expands an enterprise's attack surface.** Employees are now working outside of the bounds of the office's security infrastructure, i.e., more users are using more devices, which are connecting to a greater number of unknown and personal networking infrastructures, than ever before. Increases in remote work have put consumer internet-of-things (IoT) and mobile devices into contact with sensitive enterprise resources. And unfortunately, the end result no longer provides security teams with the same visibility and control over the devices that employees use to get work done. Decreasing efficacy of network-based security controls such as VPNs and firewalls, along with poor segmentation between sensitive devices, apps, and data, further adds to the challenges in trying to protect the expanding attack surface created by employee devices.
- **The shift to highly distributed environments opens companies up to a larger range of security risks.** Data sits at the center of any business, and the applications that access and move workloads create more access points. In addition, the increasing use of software as a service (SaaS) and cloud impacts securing applications and data.
- **Applications have reshaped data center complexity.** Most enterprises are plagued by infrastructure complexity that is driven by disparate platforms and configurations, which have accumulated over the years. As organizations trade out monolithic app architectures in favor of highly distributed microservices across multicloud environments — leveraging app containers and serverless functions — environmental complexity increases the potential blind spots for security teams trying to identify and control enterprise risks.

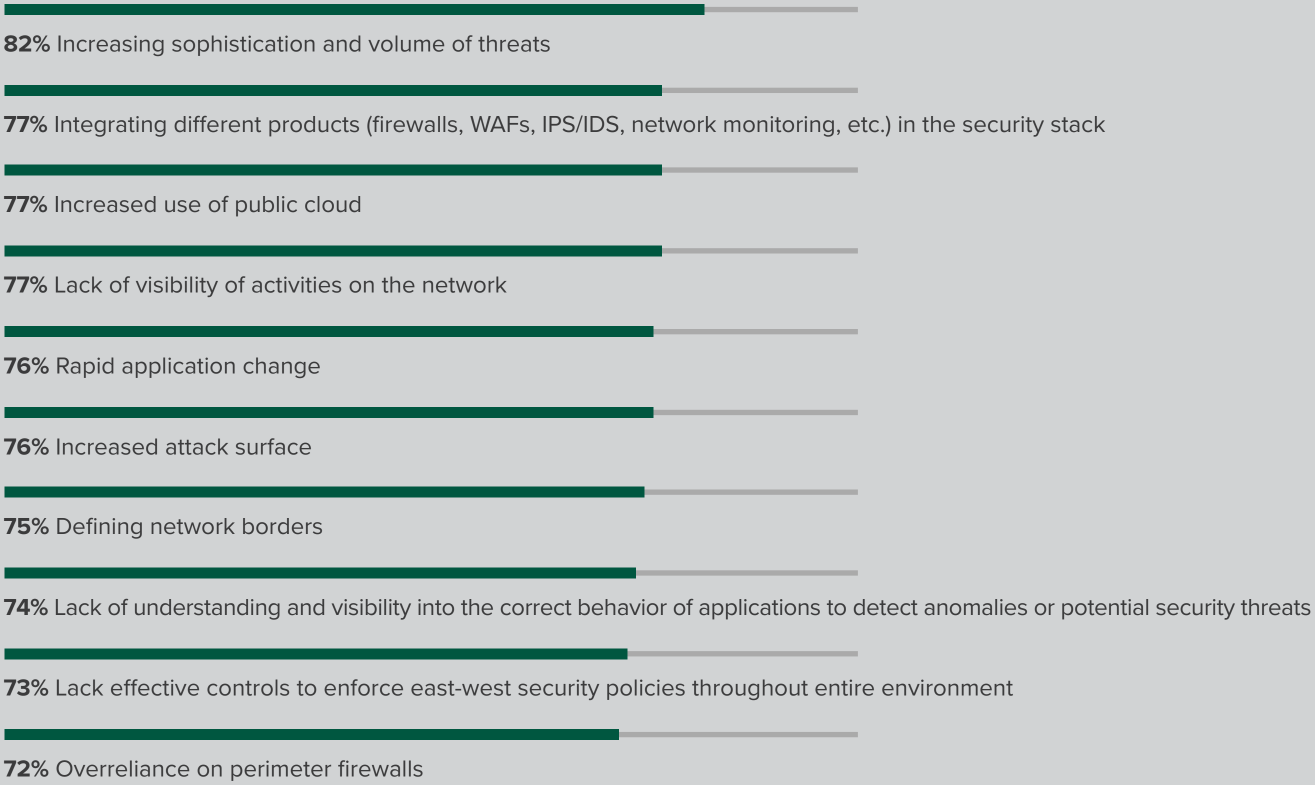
THIS SECURITY TRANSFORMATION PRESENTS BOTH TECHNICAL AND ORGANIZATIONAL/CULTURAL CHALLENGES

The transformation to a more distributed environment is challenging many enterprises as they work to secure their data, applications, and workloads. And the impact of the pandemic is only exacerbating these challenges. Recent research conducted by Forrester Consulting in partnership with VMware found these technical challenges:

› **A distributed environment clouds visibility and increases a network's attack surface.** Nearly three-quarters of IT security professionals say there's a lack of understanding and visibility into the correct behavior of applications, making it challenging to detect anomalies or potential security threats (see Figure 1).[1] In addition, more than three-quarters of enterprises report their organization is more vulnerable due to an increased attack surface.

Figure 1: Companies Face A Multitude Of Technical Challenges

"Thinking about your organization's security vulnerabilities, how challenging are each of the following technical factors?"
(Percentages represent top "moderately/very challenging")



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

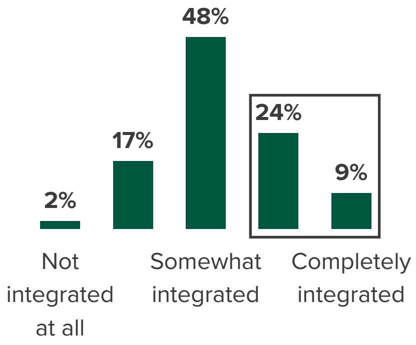
- **Too many point solutions and an overreliance on perimeter firewalls adds complexity and leaves gaps.** Seven out of 10 enterprises report an overreliance on perimeter firewalls when securing the internal network.[2] And the sheer number of security products adds complexity as more than three-quarters of companies manage 10 or more security products, while nearly 20% of companies manage 50 or more security products.[3] The multitude of these projects have either been added or bolted on over time, and they've subsequently created a patchwork that may not completely secure enterprise data and applications.
- **Disparate security solutions are creating integration challenges.** The sprawl of devices and the proliferation of different control requirements and tools compromise enterprises' security postures. It's not surprising that a majority of IT security professionals have significant integration challenges. This lack of integration hinders adaptability, creates security gaps due to misaligned controls, and makes management difficult. On average, companies have 27.4 security products. However, only one-third of respondents said their solutions are mostly or completely integrated (see Figure 2).[4]

While technical challenges are often the first identified, challenges stemming from organization and culture dynamic between senior corporate management, IT, and the security teams can have a significant impact on security enterprise data and applications. Recent research conducted by Forrester Consulting in partnership with VMware found these organizational and cultural challenges:

- **Seventy percent of enterprises lack a cohesive security strategy.** In addition, 69% report there's a lack of clear ownership over the security strategy, and 68% feel there's a lack of executive support (see Figure 3).[5]

Figure 2: Integration Of Security Solutions

"How well integrated are the security solutions in your organization?"



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Figure 3: Nearly Three-Quarters Of Companies Are Unaware Of The Risks Posed By Security Vulnerabilities

ORGANIZATIONAL CHALLENGES

74% Lack of attention/awareness of risks

73% Lack of budget

72% Lack of security staff skills

70% Lack of cohesive security strategy

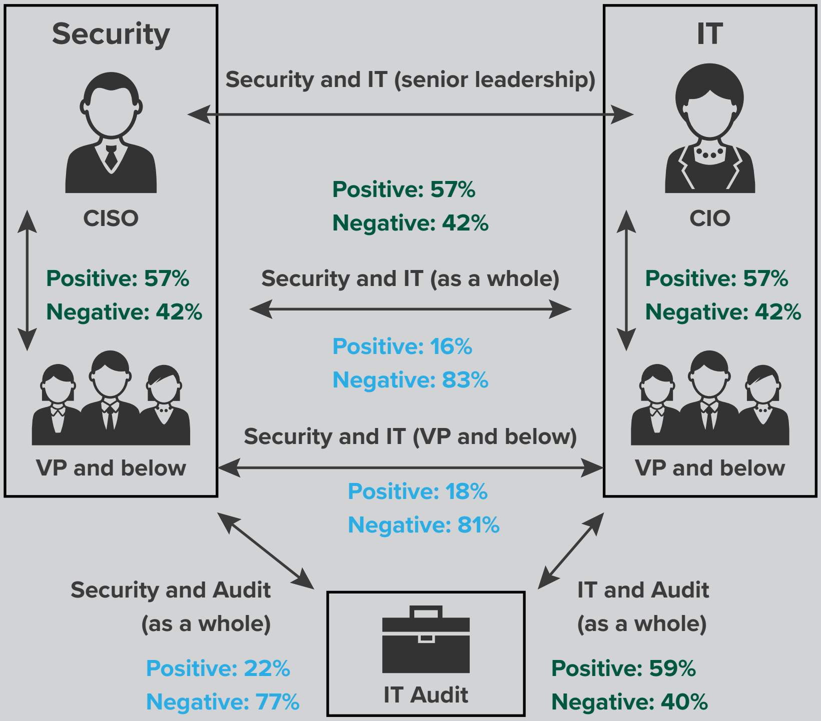
69% Lack of clear ownership of security strategy

68% Lack of executive support

Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Note: Selected variables shown.
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

- **IT leaders face pressure from the board.**[6] Our research showed that senior leadership and boards have a greater focus on security (89%) and IT (73%) than they did two years ago. CIOs and CISOs also said that the top concerns of the board include:
  - Brand protection (81%).
  - Security threats and risks to the business (78%).
  - Reducing risk and exposure (77%).
- **IT and security teams often work in silos.** These board priorities mean that CIOs and CISOs in IT and security must collaborate, despite having conflicting objectives. The push for collaboration across teams is a focus from the top down, in addition to reducing risk and protecting the company's brand, but there is clearly a cultural difference between these teams.
- **Friction between IT and security teams hinders collaboration.** In assessing these relationships, the senior-most team members had the most positive relationships, followed closely by the relationships between the two teams. The personnel of the teams were most likely to have a negative relationship with the other team (see Figure 4).[7]

Figure 4: Nature Of IT And Security Relationships



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Friction between security and IT teams hamper collaboration.

Build Your Zero Trust Strategies To Overcome Challenges

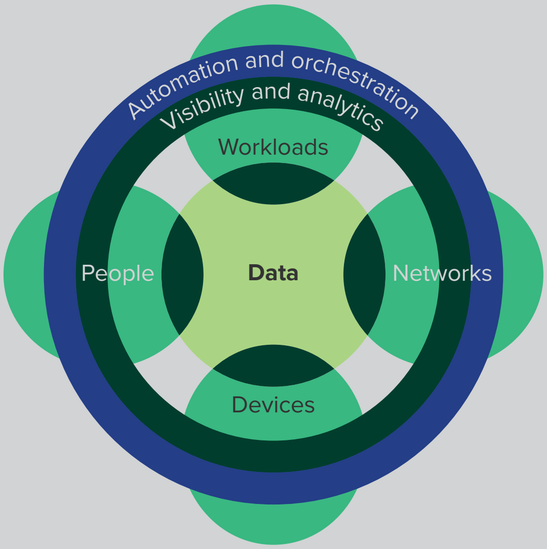
When not following Zero Trust strategies, enterprises face a wide array of challenges associated with securing their distributed environments. Forrester's Zero Trust model of information security is a conceptual and architectural model for how security teams should: 1) redesign networks into secure microperimeters; 2) use obfuscation to strengthen data security; 3) limit the risks associated with excessive user privileges; and 4) use analytics and automation to dramatically improve security detection and response.

There are seven pillars of Forrester's Zero Trust model (see Figure 5):[8]

- **Zero Trust data.** Securing and managing the data, categorizing and developing data classification schemas, and encrypting data both at rest and in transit are key to any Zero Trust approach.
- **Zero Trust users.** Limiting and enforcing user access and securing users as they interact with the internet, by continuously monitoring and governing access and privileges, is a critical component of Zero Trust.
- **Zero Trust workloads.** The workloads are front- and back-end systems that run the business and help it to win, serve, and retain customers. Just as with any other area of Zero Trust, these connections, apps, and components must be treated as a threat vector and have Zero Trust controls such as policy-based API inspection and control, container file and active memory protection, and guest host firewall. Of particular concern are workloads running in public clouds.
- **Zero Trust networks.** The ability to segment, isolate, and control the network is an important point of control for Zero Trust. Segmentation and isolation help to better secure networks.

Achieving Zero Trust is not easy, but you need to start somewhere.

Figure 5



Source: Forrester Research, Inc.

- **Zero Trust devices.** Device discovery, isolation, and management are key to controlling the risks associated with the device hardware, user behavior, apps, and data accessed from the device.
- **Visibility and analytics.** The security analyst needs to have the ability to accurately observe threats that are present and orient defenses more intelligently.
- **Automation and orchestration.** Organizations and security leadership need to use tools and technologies that enable security automation and orchestration (SAO) across the enterprise, to shorten incident response times and integrate disparate security solutions. Orchestration extends security policies to cloud environments.

HOW TO ACHIEVE ZERO TRUST SUCCESS

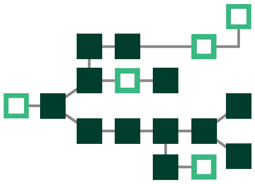
To improve effectiveness of your Zero Trust efforts, there are two things to do: 1) implement solutions with intrinsic security and 2) alleviate organizational and cultural issues hampering collaboration between the IT and security teams.

Recent research conducted by Forrester Consulting in partnership with VMware found the following:

- **Intrinsic security minimizes the remaining risk of technical failure.** Intrinsic security solutions are built-in, software solutions that help companies reduce their threat vectors by being built-in versus bolted on, by unifying tools and teams to improve visibility, and by using real-time context to better detect and respond to threats.
- **Intrinsic security reduces complexity and costs.** Faster investigation and remediation and reduced complexity driven by intrinsic security ultimately lead to reduced capital and operational expenditures.
- **Increase your chances for success by making Zero Trust a collaborative activity.** Zero Trust success hinges on the entire organization focused on the same objective, with IT and Security professionals working in partnership. Break down the IT and Security siloes by bringing the teams together to set agreed upon goals, objectives and measures of success.

Steps To Take On Your Zero Trust Journey

Creating a detailed roadmap that outlines the main workstreams and projects necessary to implement your Zero Trust strategy is critical for success. A good Zero Trust roadmap shows exactly what you plan to deliver, how much your executives will need to invest, and what specific business and security outcomes will be achieved.

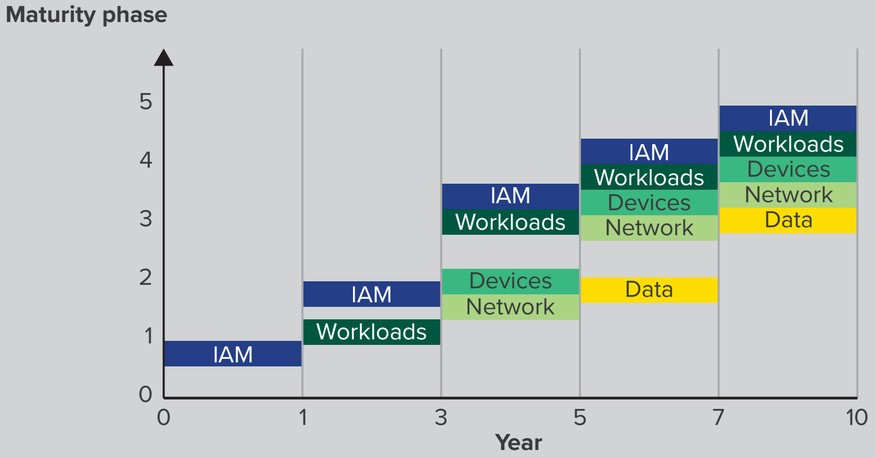


- **Security and IT must work with the business together.** Identify key players that are critical to the Zero Trust strategy; include a board member if you can, IT executives (where budget will come from), and enterprise architects and application owners, who will ensure Zero Trust supports the broader IT strategy, which in turn will support the broader business strategy.
- **Identify interdependencies.** A Zero Trust effort needs to include existing security, IT, and business projects in order to succeed. Cloud migration, network modernization, and partner onboarding can be catalysts for a Zero Trust transformation. Ensure that you are properly mapping and clearly communicating project dependencies.
- **Assess and goal Zero Trust maturity.** Conduct a Zero Trust security assessment of your current capabilities and then set a desired future state maturity (see Figure 6). From there, you can build a roadmap of technological and process progression around the seven pillars of the Zero Trust extended ecosystem: data, people, devices, networks, workloads, visibility and automation. Forrester recommends at least a two- or three-year horizon overall (see Figure 7).

As remote work moves into being a prolonged effort, companies are going back and securing their distributed employees, devices, and enterprise applications using a combination of security and IT management. Both IT and security leadership want to find ways to reduce environmental complexity and increase teams' efficiency and precision.

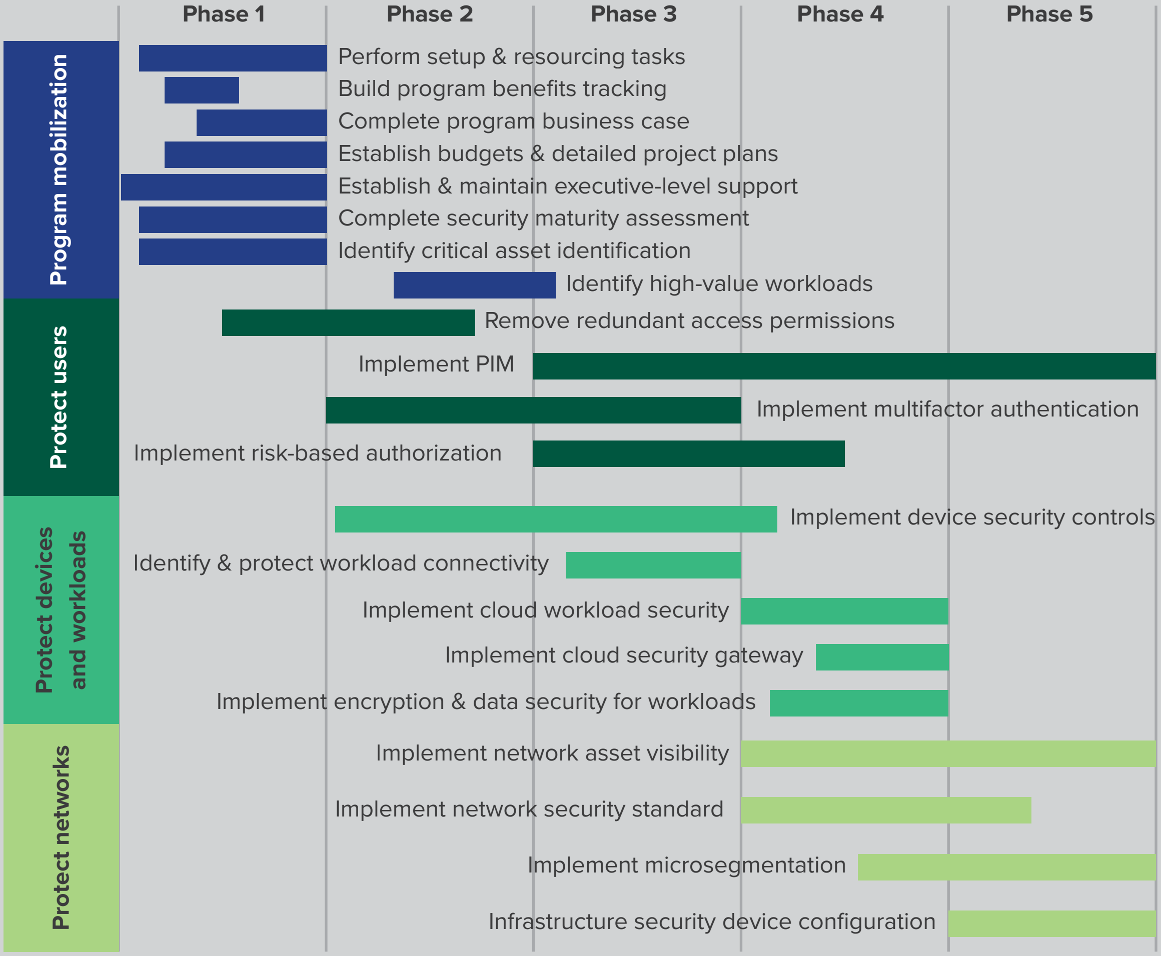
While technology solutions are partly the answer, many companies are facing both pressure from the board and collaboration challenges between IT and security teams. Forrester's Zero Trust strategies can provide a roadmap to overcome these challenges. And in combination with intrinsic security solutions, companies can quickly find and remediate security vulnerabilities.

Figure 6: Sample Desired Future State Maturity



Source: Forrester Research, Inc.

Figure 7: Sample Zero Trust Roadmap

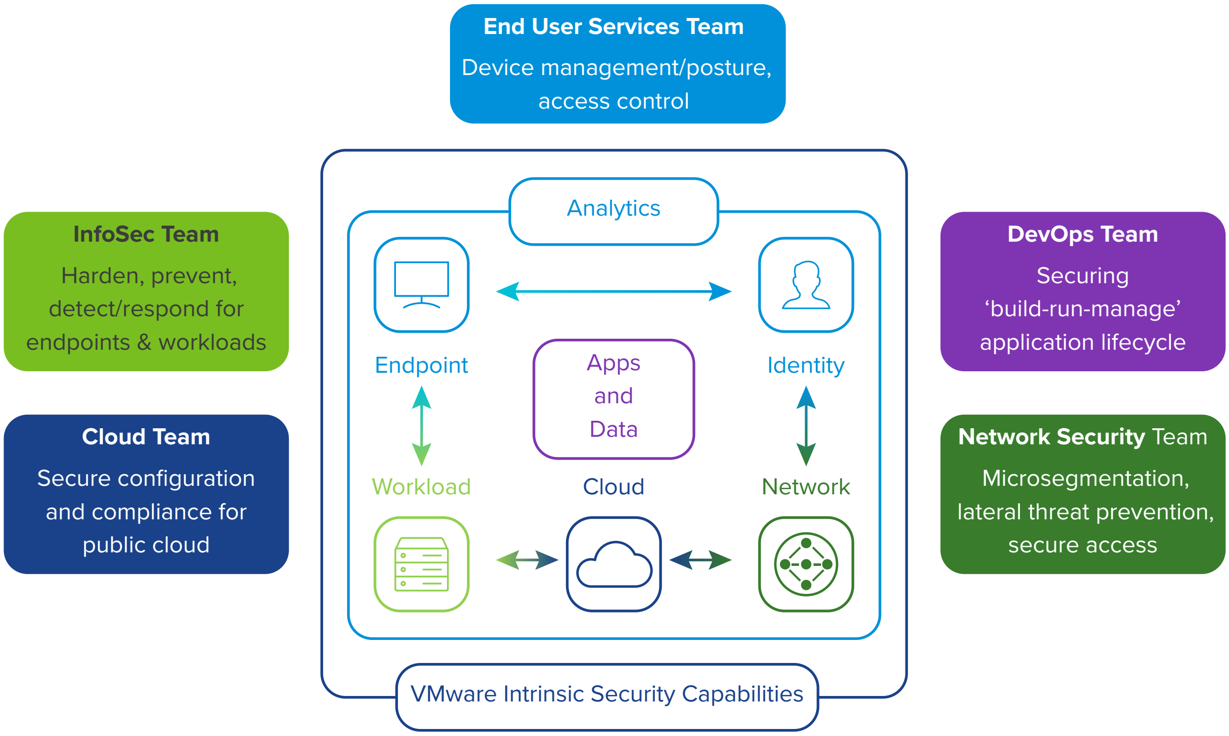


Source: Forrester Research, Inc.

VMware Intrinsic Security

The following information is provided by VMware. Forrester has not validated any claims and does not endorse VMware or its offerings.

VMware's intrinsic security approach leverages your existing VMware infrastructure as security control points providing visibility into networks, endpoints, user identities, cloud infrastructure, and workloads. By using a built-in vs bolt-on approach, tools and teams can be unified reducing complexity and costs. The improved cross-team visibility can help IT and security work in partnership supporting a collaborative approach to Zero Trust.



End User Services Team
Device management/posture, access control
InfoSec Team
Harden, prevent, detect/respond for endpoints & workloads
Cloud Team
Secure configuration and compliance for public cloud
DevOps Team
Securing 'build-run-manage' application lifecycle
Network Security Team
Microsegmentation, lateral threat prevention, secure access
Analytics
Endpoint
Identity
Apps and Data
Workload
Cloud
Network
VMware Intrinsic Security Capabilities

Data

VMware verifies every access to data with authentication and authorization at device and network level. VMware's storage solutions provide built-in encryption for data at rest.

Users And Devices

VMware brings together unified endpoint device management, conditional access, and intelligence capabilities for establishing continuous authentication and enforcement of access policies. Administrators can allow access from only permitted compliant devices. Once device compliance is established, a range of access policies can be set incorporating location, application, and risk analytics while end users seamlessly authenticate via a range of different modern authentication methods for verified access to applications and data. Additionally, cloud native endpoint protection combines threat detection and behavioral protection to further strengthen security.

Workloads

For workloads, VMware provides visibility and analysis of configuration, state, and vulnerabilities for hardening; prevention mechanisms against malware, ransomware, and non-malware/file-less attacks; and detection and response mechanisms for attacks that circumvent both of those processes and controls. It covers workloads in private and public clouds, for both traditional virtual machines and Kubernetes containers. Their approach can also leverage some unique integrations with the virtual fabric that enable it to be agentless on vSphere (and a single lightweight sensor in other environments), and integrated with vCenter — providing a single source of truth to both security and infrastructure teams. That enables better collaboration between security and IT, and more effective operationalization of workload security through the infrastructure team. Combined with the NSX microsegmentation technology, it can set up a Zero Trust posture from both the workload and network standpoint — both aligned to the applications they serve.

Networks

VMware's distributed approach to firewalling goes from macro to microsegmentation offering stateful L7 controls and advanced threat prevention. Its unique distributed architecture requires no network changes. Built into the hypervisor, the distributed firewall platform has complete visibility into application topology and automatically formulates microsegmentation policies. A single solution provides consistent policy across virtualized, containerized, and bare metal workloads spanning private and public cloud environments.

With network security and access controls built into the SD-WAN architecture with global POP locations, VMware enables Zero Trust network access for users from anywhere to applications in multicloud locations.

Analytics

VMware solutions include built-in analytics to provide complete visibility and alerting to security operators. In additional to the built-in analytics, VMware Threat Analysis Unit (TAU), a central team of threat researchers and data scientists, leverages product telemetry, partner feeds, and AI techniques to ensure the platforms are powered with best threat intelligence and up-to-date algorithms.

Orchestration And Automation

VMware solutions feature orchestration options across workload, device, and networking. Detailed visual workflows can be constructed to automate tasks including workload deployment, network segmentation, device provisioning, and threat isolation.

Forrester Total Economic Impact Studies Commissioned By VMware

Total Economic Impact (TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The objective of the TEI framework is to identify the cost, benefit, flexibility, and risk factors that affect investment decisions.

VMware commissioned Forrester Consulting to conduct the following recent TEI studies:

The Total Economic Impact™ Of VMware NSX[9]	**ROI: 95%**	**Payback: <12 months**
The Total Economic Impact™ Of VMware Carbon Black Cloud[10]	**ROI: 379%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware vRealize Network Insight[11]	**ROI: 477%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware End User Computing[12]	**ROI: 152%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware Workspace ONE[13]	**ROI: 206%**	**Payback: <6 months**
The Total Economic Impact™ Of VMware Workspace ONE For Windows 10[14]	**ROI: 139%**	**Payback: 7 months**

Appendix A: Supplemental Material

RELATED FORRESTER RESEARCH

"Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model," Forrester Research, Inc., July 2, 2020.

"The Zero Trust eXtended (ZTX) Ecosystem," Forrester Research, Inc., July 11, 2019.

Appendix B: Endnotes

[1] Source: "To Enable Zero Trust, Rethink Your Firewall Strategy," a commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020.

[2] Source: Ibid.

[3] Source: Ibid.

[4] Source: Tension Between IT And Security Professionals Reinforcing Silos And Security Strain, May 2020

[5] Source: "To Enable Zero Trust, Rethink Your Firewall Strategy," a commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020.

[6] Source: Tension Between IT And Security Professionals Reinforcing Silos And Security Strain, May 2020.

[7] Source: Ibid.

[8] Source: "A Practical Guide To A Zero Trust Implementation," Forrester Research, Inc., January 15, 2020.

[9] Source: "The Total Economic Impact™ Of VMware NSX," Forrester Consulting report prepared for VMware, May 2020.

[10] Source: "The Total Economic Impact™ Of VMware Carbon Black Cloud," Forrester Consulting report prepared for VMware, May 2020.

[11] Source: "The Total Economic Impact™ Of VMware vRealize Network Insight," Forrester Consulting report prepared for VMware, July 2019.

[12] Source: "The Total Economic Impact™ Of VMware End User Computing," Forrester Consulting report prepared for VMware, April 2019.

[13] Source: "The Total Economic Impact™ Of VMware Workspace ONE," Forrester Consulting report prepared for VMware, October 2018.

[14] Source: "The Total Economic Impact™ Of VMware Workspace ONE For Windows 10, Forrester consulting report prepared for VMware, October 2018.