

## Palo Alto Networks Cloud-Delivered Security Services Enhance Security And Compound Benefits Of Other Network Security Investments

As network architecture becomes more complex, security teams increasingly struggle to adapt and provide consistent security to all devices and data traversing their networks and clouds. Subscription-based security services are a growing piece of most organizations' security strategies, enabling rapid scalability of protection with up-to-the-minute updates and simplifying the deployment and management of security. While price is a primary concern for many organizations, firms must also consider the specific capabilities of each existing and new security product to evaluate how those services integrate with and amplify the efficacy of existing systems and workflows.

Forrester recently spoke with multiple Palo Alto Networks customers regarding their investment in the range of Cloud-Delivered Security Services. Forrester conducted these conversations as part of a Total Economic Impact™ (TEI) study to understand the value and impact of these services on a customer's total security strategy.

Organizations find themselves with a myriad of security point solutions and services designed to address specific needs. Resource constraints and other factors prevent them from fully realizing both the value and capabilities of many of these pieces.

Some **key challenges** include:

- Successfully managing sprawling security solution stacks with multiple vendors, platforms and overlapping capabilities.
- Integrating cloud-delivered point services, new appliances, or network configurations

### Benefits Related To Cloud-Delivered Security Services



Time to attain proper security posture compared to using point solutions  
**30% faster**



Reduced risk of a security breach  
**45%**



Security infrastructure cost savings from a common platform vs. point solutions  
**\$9.9 million**

with existing cloud or on-premises networks and systems.

- Tuning security measures, processes, and policies effectively and efficiently to minimize gaps while maintaining control.
- Analyzing and tracking gaps between multiple vendors with similar products deployed into different infrastructure.

Beyond this, Forrester also found that speed matters — especially when it pertains to defending against attacks that depend on extended dwell times to proliferate east and west across the network. Live services make the difference on an order of magnitude for reducing organizational risk.

The primary services discussed in the study include intrusion detection and prevention systems (IPS/IDS), malware analysis and sandboxing, web security

(secure web gateway [SWG] technology, DNS security), software-as-a-service (SaaS) security (cloud access security broker [CASB]), and internet-of-things (IoT) security.

To address the key challenges above, organizations looked for a unified security solution that:

- Automatically shared intelligence to provide in-depth defense.
- Integrated all existing infrastructure (hardware, software, cloud and subscription services) into a single platform.
- Was managed from a single pane of glass with a similar look-and-feel.

Palo Alto Networks offers multiple Cloud-Delivered Security Services that are specifically designed to complement and enhance each other and ensure that customers can confidently secure all traffic that transverses any networks or clouds. Additionally, these security capabilities aid and support the Zero Trust model for network security initiatives.

This spotlight focuses exclusively on the interviewed organizations' use of the following Palo Alto Networks Cloud-Delivered Security Services, their value, and their impact to the organizations:

- [Threat Prevention](#) (for IPS).
- [WildFire](#) (for malware analysis and sandboxing).
- [URL Filtering](#) and [DNS Security](#) (for web security or SWG).
- [IoT Security](#) (for IoT, IoMT, and OT security).
- [Prisma SaaS](#) (CASB or SaaS security).

These solutions are combined with Palo Alto Networks Next-Generation Firewalls (NGFW), VM-Series, and Prisma Access for consistent security delivered across all locations including, HQ, data center, branch offices, and remote workers.

For a description of each Cloud-Delivered Security Service, please reference the [Product Glossary](#).

## KEY RESULTS

The high-level key results from the TEI study include:

### **\$6 million in efficiency gains for security operations and end users.**

Security operations center (SOC) teams were able to reduce the number of advanced investigations by 35%, improve mean-time-to-resolution (MTTR) by 20%, and cut the number of devices that require reimaging by 50%. End users shared in these benefits through fewer and faster interactions with their security teams.

### **\$9.2 million in savings enabled by a 45% data breach risk reduction.**

Each of the Palo Alto Networks Cloud-Delivered Security Services seamlessly integrates with and enhances the capabilities of the ML-Powered (Machine Learning-Powered) NGFW deployment, improving network security coverage and capabilities while protecting the entirety of the attack surface. When a data breach happens, organizations must deal with a myriad of costs. Palo Alto Networks Cloud-Delivered Security Services help prevent the incident from happening from the onset, which also helps mitigate any follow-on costs that might occur.

- **Reduce threats related to employee devices and activities.** With Palo Alto Networks' Cloud-Delivered Security Services adherence to the Zero Trust model, organizations are better protected from both external and internal threats, with different services working together to constantly monitor web traffic, application traffic, data in SaaS applications, user- and entity-based analytics, data exfiltration, and zero-day exploits and malware. Better protection leads to fewer incidents, which in turn translates to improved uptime for systems and employees.
- **Mitigate coordinated attacks to applications, servers, and site locations.** With the latest in detection algorithms, signatures, and inline machine-learning capabilities shared among the products, Palo Alto Networks' Cloud-Delivered Security Services can analyze a newly discovered threat in one part of the organization

of a single customer, unpack its components, share the intelligence across security services and distribute prevention in seconds so that any other location or customer can be safely protected from that zero-day or variant at any point in the attack lifecycle. As a simple example, new malware that attempts to connect to an unknown domain is automatically analyzed, and as a result, the Threat Prevention, WildFire, URL Filtering, and DNS Security solutions all receive updates from this intelligence, creating future prevention of the technique and each individual tactic for every customer going forward. This unique aspect provides much improved coverage at a foundational level for zero-day exploits and threats over legacy and siloed cloud-based point solutions.

**\$9.9 million in security infrastructure cost reduction and avoidance and an additional \$1.9 million from security stack management efficiencies that reduce workloads by almost 50%.**


With Palo Alto Networks Cloud-Delivered Security Services, organizations can rationalize and remove a large portion of their legacy security stack, reducing the number of vendors in their environment and the number of security licenses needed to protect their networks.

- **Reduce complexity to reduce management effort.** Interviewees' organizations could reallocate almost half of their security infrastructure management teams due to the efficiencies afforded by Palo Alto Networks Cloud-Delivered Security Services seamless integration with Panorama, the Palo Alto Networks network security management tool, for a consistent look-and-feel across all products. Management teams could shift left to eliminate advanced investigation work, reduce the effort involved with updates and patching, and minimize effort associated with policy and data management with a centralized location to manage all security policies.

A head of IT architecture in the technology manufacturing industry said: "I now have more consistent security policy across my entire infrastructure worldwide. I don't have different vendors with different policies and different updates. I've got a lot more consistency. It goes back to the single pane-of-glass, but even without that, I've got a security policy that I know if I can define it once, I can run it everywhere."

- **Common platform reduces the number of vendors and security licenses, allowing organizations to consolidate and rationalize their security stack.** By providing a comprehensive security suite of products and capabilities that all feed into a centralized platform, organizations could significantly reduce the cost of their security stacks, eliminate point solutions, and reduce the number of vendors and disparate technologies in their environments. Another benefit to this consolidation is that because Palo Alto Networks Cloud-Delivered Security Services and NGFWs are designed to work together, interviewees reported having better coverage of their entire networks from data centers to endpoints at remote locations.

Reallocate **half of the security infrastructure management team** with Cloud Delivered Security Services and Panorama.



**\$1.4 million in savings on IoT from reduced management effort and a reduction in the number of new IoT devices purchased.** With IoT Security, organizations could identify and secure all their IoT devices from a central platform, quickly understand the health and location of each device, and maximize the value and utilization of each device with the enhanced reporting capabilities. This reduced spend on new device purchases by 10%.

[→ READ THE FULL STUDY HERE](#)

**\$812K in savings from faster security posture attainment speed with Palo Alto Networks, freeing up more time for enhancements.**

Organizations experienced reduced deployment and fine-tuning times with Palo Alto Networks. Native integration with the NGFW, VM-Series, and Prisma Access deployments and complementary management capabilities made it easier for organizations to reach steady state for their security solutions.

A senior director of cybersecurity in the entertainment industry said: “Much less training equates to much more consistent and rapid care and feeding of the solution overall. My team is able to keep things

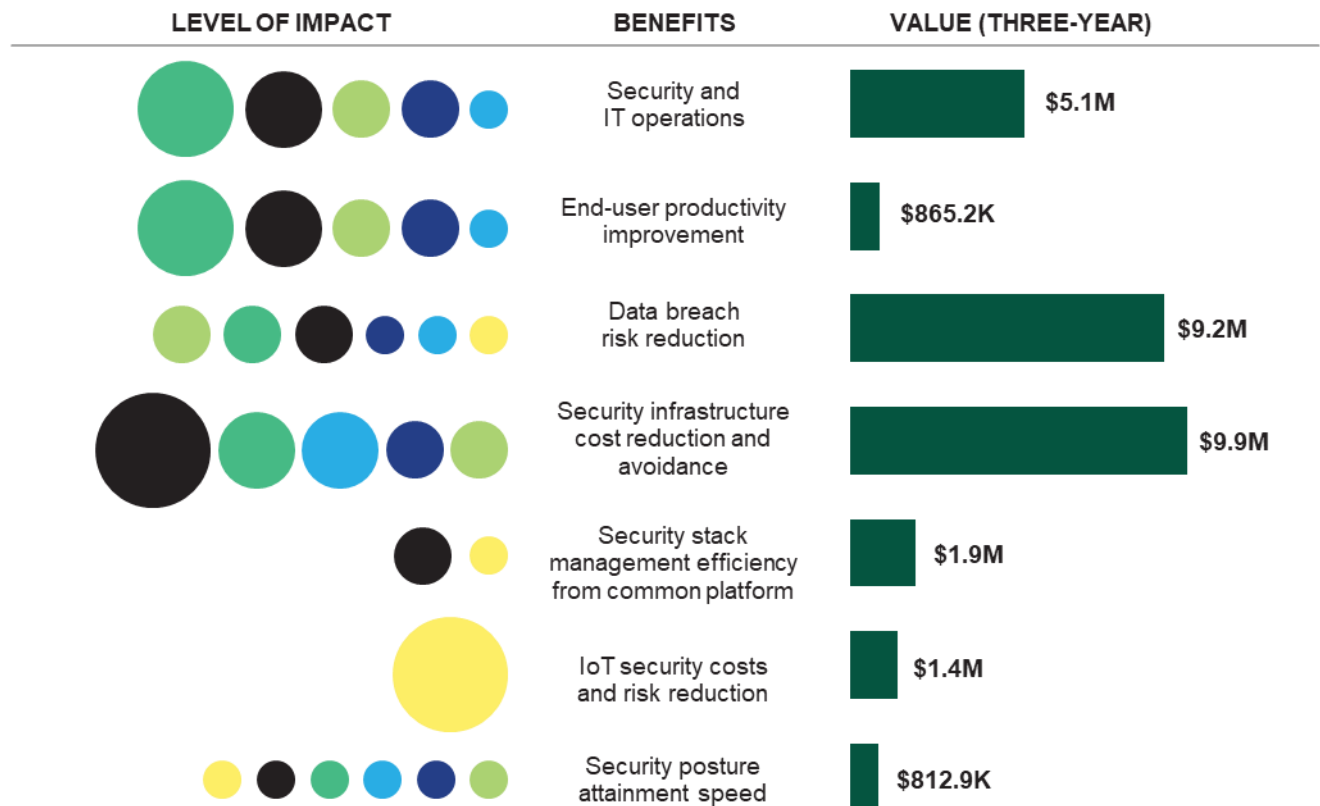
current more easily, and that is important because the bad guys are constantly innovating.”

- **Less time training, maintaining, and investigating means more time advancing projects and adding value to the organization.**

A lead network architect in the retail/manufacturing industry explained: “We are doing a lot more projects since moving to Palo Alto Networks. We have several big projects we are doing this year that we simply did not have the resources to complete in the past. With Palo Alto Networks, we’re spending a lot more time on projects and a lot less time on day-to-day care and feeding.”

**Relative Impact Of Palo Alto Networks Cloud-Delivered Security Services**

**Subscriptions**



Source: Benefit calculation tables from “The Total Economic Impact™ Of Palo Alto Networks For Network Security And SD-WAN,” a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, November 2020

## THE IMPACT OF EACH CLOUD-DELIVERED SECURITY SERVICE

Below is a description of each Cloud-Delivered Security Service along with its relative impact on the quantified benefits listed above.

**Prisma SaaS provides security and compliance for SaaS environments and cloud data.** Prisma SaaS enables safer cloud adoption by providing visibility, compliance controls, and security across SaaS applications and sensitive data. It helps organizations minimize the use of shadow IT, secure corporate SaaS applications, mitigate the risk of a breach or accidental data exposure in the cloud, and enhance data privacy and compliance.

With Prisma SaaS, organizations get consistent cloud security and data protection across sanctioned and unsanctioned SaaS applications. As an integrated part of Palo Alto Networks security, it is a service tightly embedded the broader companywide cybersecurity program, providing a streamlined deployment that allows overcoming the piecemeal approach of point controls like CASB and SaaS built-in security capabilities.

**Securing web access reduces alerts and investigations.** URL Filtering detects and blocks any web-based threats, feeding alerts and data into Panorama, for secondary analysis and policy review if required. Palo Alto Networks URL Filtering enables users to safely access the web by protecting them from phishing attacks, malware, exploit kits, and other forms of malicious websites. The URL Filtering service natively integrates with all physical, virtual, and cloud-delivered NGFWs, so security teams only need to manage and deploy a single policy set.

With URL Filtering, organizations reduce the number of security incidents requiring advanced investigations, reduce the likelihood of a data breach, and sunset legacy web security technologies.

**WildFire protects assets from zero-day threats.** WildFire provides cloud-based malware detection and sandboxing with real-time updates to protect against highly evasive and previously unknown

threats, including fast moving polymorphic malware. In addition to real-time streaming of updates, WildFire powers an inline machine-learning capability that blocks most new file-based threats instantly. WildFire quickly became a key piece of the interviewed organizations' security posture by offering immediate protection, distributing intelligence to enhance other services, reducing events per analyst hour with detailed insight into the behavior of identified threats, and feeding actionable alerts to the SOC.

With WildFire, organizations improve efficiency for IT and SOC teams, reduce the likelihood of a data breach, and sunset legacy sandboxing technology.

**DNS Security blocks malicious domains and applies predictive analytics to disrupt attacks that use DNS for command and control or data theft.** The solution monitors DNS traffic and prevents tunneling, domain-generation algorithms, and other DNS-based threats that could allow attackers to spread east-west across the network.

DNS Security prevents threats at the DNS level before they can do damage, taking the burden of reaction time off your other security devices and people resources.



**Reduce annual spend on new IoT devices**

**10%**

**Threat Prevention stops known threats and vulnerabilities sooner.** Threat Prevention from Palo Alto Networks incorporates IPS and threat scanning capabilities to prevent all known threats and vulnerabilities across all traffic in a single pass. It further enhances the capabilities of NGFW deployments by automatically delivering the latest threat intelligence to all NGFWs from factors. Exploits, spyware, malware, and other threats are prevented at an early stage to avoid infection and downstream creation and investigation of alerts. Working in conjunction with WildFire for unknown threat prevention, Threat Prevention can block malware sooner with preventions shared across all

security controls to harden the security posture in near-real time.

With Threat Prevention, organizations reduce the number of security incidents requiring advanced investigations, reduce the likelihood of a data breach, and sunset legacy IPS solutions.

**IoT Security reduces management effort and extends device lifecycles.** Palo Alto Networks IoT Security integrates with Palo Alto Networks NGFWs, VM-Series, and Prisma Access management console, providing organizations with a single place to view and manage policy for all IoT devices. After deploying IoT Security, interviewed organizations could easily track down previously unknown or lost devices for segmentation and monitor all device traffic. Additionally, Palo Alto Networks IoT Security provided recommended trust policies to more easily apply security controls to IoT devices, improving organizational security, reducing the attack surface for potential bad actors, and more accurately controlling risk.

**“I now have more consistent security policy across my entire infrastructure worldwide.”**

*Head of IT architecture, technology*

## WHY ORGANIZATIONS SELECTED PALO ALTO NETWORKS CLOUD-DELIVERED SECURITY SERVICES

Interviewees shared several reasons for selecting Palo Alto Networks Cloud-Delivered Security Services, including:

- **Seamless integration into a single pane of glass with Palo Alto Networks Panorama.** All of these services seamlessly integrate with the NGFW and Panorama, Palo Alto Networks' centralized management platform, reducing the workload for IT and the SOC team by providing a common platform with a common interface for all security technology and services. A network security manager in the retail industry said, “We consider URL Filtering to be a big part of our

security posture, and WildFire-based alerts are extremely actionable.”

A senior VP in the financial services industry explained: “Our top benefit has been our improved security posture especially around internet access. With Palo Alto Networks, we can identify what traffic is actually going on, only allowing what we actually care about and blocking everything else whether it be URL- or application-based.”

A VP of cybersecurity in the entertainment industry added: “One of the top benefits is the commonality of the platform. Somebody who is administering Prisma SaaS, Prisma Cloud, all those different things have a similar look-and-feel. Now, I don't need to send people to different trainings to figure out how to use our tools. And everything else is in Panorama so Threat Prevention, WildFire, URL Filtering, DNS Security, the firewall policies, and decrypt rules all exist in Panorama. It all comes back to that common user-interface model.”

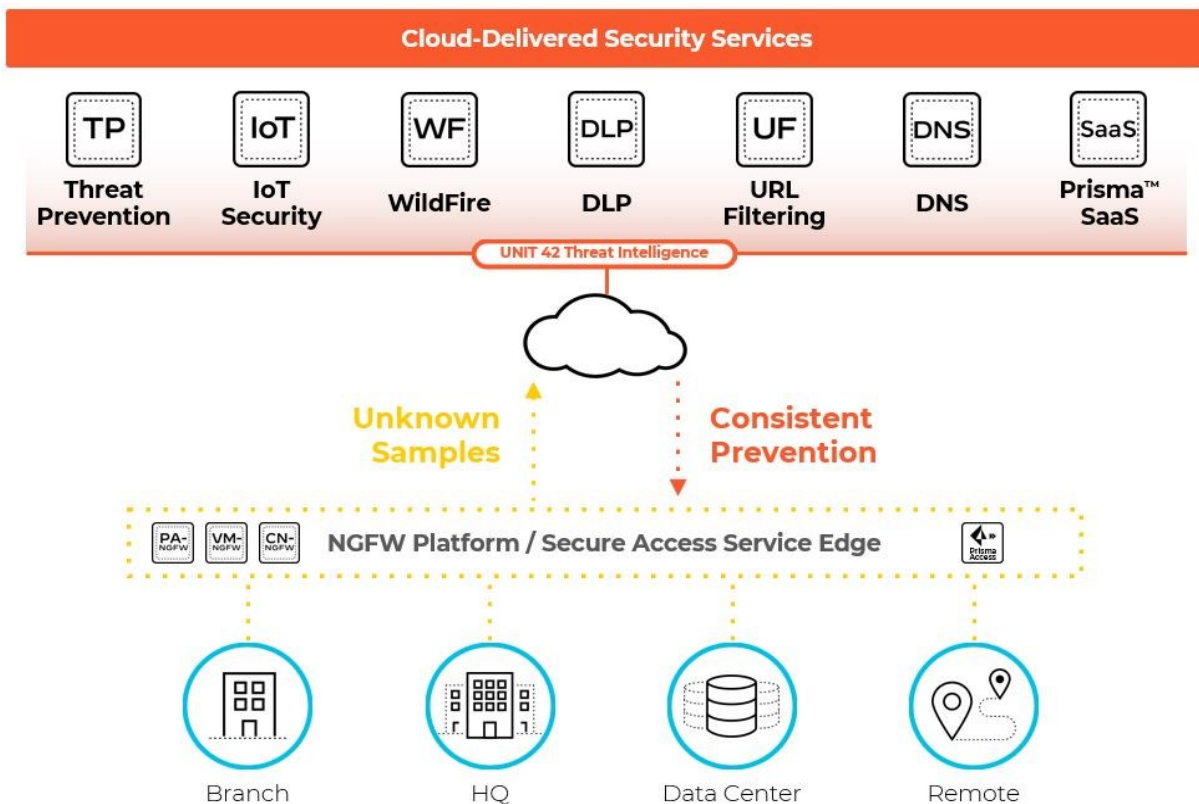
- **Security without performance compromise.** Interviewees noted that the security industry in general is moving toward a subscriptions-based services model and that Palo Alto Networks technology, with its parallel processing capabilities, is specifically engineered to outperform competitors in that type of environment. Additionally, with Palo Alto Networks inline machine learning, the security offerings are continuously improving and providing better protection.

A CISO in the retail industry said: “We knew that moving forward, the security industry is going to rely on more subscriptions being tied to existing hardware so that is the assumption that we operated under. Palo Alto Networks is the only firewall out there that is engineered with parallel processing architecture so with all the features turned on, which is how we intend to operate, there was no drop in performance like we saw with the other technologies.”

# Glossary: Palo Alto Networks Products

The following information is provided by Palo Alto Networks. Forrester has not validated any claims and does not endorse Palo Alto Networks or their offerings.

- **CLOUDGENIX SD-WAN:** Application defined and autonomous next-generation SD-WAN solution that enables the cloud-delivered branch.
- **DNS SECURITY:** A cloud-delivered service that applies predictive analytics to disrupt attacks that use DNS for C2 or data theft as they occur.
- **ENTERPRISE DATA LOSS PREVENTION (DLP):** The industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across every network, cloud, and user. (Enterprise DLP was not included in the TEI analysis.)
- **IOT SECURITY:** The industry's only complete IoT security product with visibility, prevention, and enforcement for every IoT and OT device.
- **NEXT-GENERATION FIREWALLS (NGFW):** Industry-leading family of physical (PA-Series), virtualized (VM-Series) and containerized (CN-Series) firewalls that leverage machine learning for proactive protection.
- **PANORAMA:** Centralized network security management solution for your Palo Alto Networks Next-Generation Firewalls — all form factors and all locations.
- **PRISMA ACCESS:** A secure access service edge (SASE) solution for networking and security in a purpose-built cloud-delivered infrastructure.
- **PRISMA SAAS:** Comprehensive visibility, security, and compliance across the industry's broadest range of SaaS applications and your data within.
- **THREAT PREVENTION:** The market-leading advanced intrusion prevention system (IPS) inspects all traffic for threats and automatically blocks known vulnerabilities.
- **UNIT 42:** Palo Alto Networks' global threat team, the recognized authority on cyberthreats, delivers insights to security teams and sophisticated protections across the product portfolio by conducting in-depth research on threat actors, their tools, techniques, and procedures.
- **URL FILTERING:** Cloud-delivered web security that protects against web-based threats such as phishing, malware, and command-and-control.
- **WILDFIRE:** Industry's leading advanced malware analysis engine that identifies and protects against unknown file-based threats.



## ADDITIONAL RESOURCES

Forrester developed additional resources to dive deeper into the impact and benefits of the specific solutions included in this study. More information and access to these additional resources can be found here:

- [The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN](#)
- [Executive Summary: TEI™ of Palo Alto Networks for Network Security and SD-WAN](#)
- [TEI Spotlight: CloudGenix SD-WAN](#)
- [TEI Spotlight: Prisma Access](#)

### TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full report “The Total Economic Impact™ Of Palo Alto Networks For Network Security And SD-WAN,” commissioned by Palo Alto Networks and delivered by Forrester Consulting.

### STUDY FINDINGS

Forrester interviewed nine decision-makers at separate organizations with experience using the Palo Alto Networks NGFWs and Cloud-Delivered Security Services and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Security and IT operations efficiency gains including a 35% reduction in security incidents requiring advanced investigations and a 20% reduction in MTTR totaling \$5.1 million.
- Data breach risk reduction of 45%, saving \$9.2 million.
- Security stack infrastructure cost avoidance and management efficiencies totaling \$11.7 million.



**Return on investment (ROI)**

**247%**



**Net present value (NPV)**

**\$28.5 million**

## DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Palo Alto Networks and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Palo Alto Networks.
- Palo Alto Networks reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester’s findings or obscure the meaning.
- Palo Alto Networks provided the customer names for the interviews but did not participate in the interviews.

## ABOUT TEI

Total Economic Impact™ (TEI) is a methodology developed by Forrester Research that enhances a company’s technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. 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 TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.



FORRESTER®