Implementing Zero Trust

A Forcepoint guide for agencies

Forcepoint

Whitepaper

Forcepoint
May 21, 2020
Zero Trust

forcepoint.com

Table of Contents

Federal security transformation

Infrastructure-centric security deployed today divides enterprise users into two domains, trusted users on the inside and untrusted individuals on the outside. Security leaders are focused on deploying controls to keep the untrusted individuals out. However, digital transformation and multi-cloud adoption by enterprises force organizations to rethink the traditional network perimeter. As users, partners, and customers access the organization's data from anywhere in the world, the artificial wall that protects the data is no longer enough, and inherent trust can't be part of the security stack going forward.

Federal cybersecurity is at a critical juncture. Networks are growing in size and complexity, requiring massive amounts of rapid data transfer to maintain situational awareness on the digital and physical battlefield. This expansion is stretching existing cybersecurity apparatuses to their breaking point, as an ever-growing number of users and endpoints increases the attack surface of the network. This challenge is not unique to the federal government—the commercial sector is facing the same challenges as their networks are constantly increasing connections to a broad range of other networks that drive new vulnerabilities. Blind trust in users and devices inside the perimeter of the network is not sustainable and will continue to put national security information and operations at risk until it is resolved. As a result, public and private sector organizations are reassessing the current method of "perimeter" security and are considering new methods. One such method is "zero trust," which could drive a step-change in security improvement across commercial and federal networks. Zero trust architectures (ZTAs) can significantly offset vulnerabilities and threats across government networks by creating discrete, granular access rules for specific applications and services within a network.

Forcepoint has a long history of working with commercial and government customers to develop effective, risk-based programs to protect data, intellectual property, and information systems. This document provides organizations an overview on the fundamentals of zero trust, and details why agencies must think beyond identity as they develop a robust mitigation program to improve an enterprise's overall cybersecurity posture.

Inherent trust of users inside your network is no longer working, causing federal users to consider whether zero trust architectures can help solve modern security challenges.

Zero Trust Architectures

The definition of zero trust has evolved greatly over the past 10 years

The zero trust security framework was first developed by Forrester Research analyst Jon Kindervag in 2009. The initial framework treated all network traffic as untrusted and recommended that organizations inspect all traffic and divide the network into small segments. Since 2009, the framework has evolved into advocating for the need to protect the organization's data and evaluate access to the data throughout the user and device interaction. In simple terms, the core principle of zero trust is to "never trust, always verify." In 2020, the definitions and guidance for what zero trust is and how it should be implemented have been formally laid out in the pending NIST 800-207 publication.

NIST tenets of a zero trust architecture

NIST defines zero trust as the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources. A ZTA uses zero trust principles to plan enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet). Authentication and authorization (for both user and device) are discrete functions performed before a session connecting to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. Today's zero trust focuses on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

.

According to NIST, a zero trust architecture must be designed and deployed with adherence to the following zero trust basic tenets:

1. All data sources and computing services are considered resources.

A network may be composed of several different classes of devices. A network may also have small-footprint devices that send data to aggregators/storage, software-as-a-service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

2. All communication is secured regardless of network location.

Network location does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a traditional network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.

3. Access to individual enterprise resources is granted on a per-session basis.

Trust in the requestor is evaluated before the access is granted. This could mean only "sometime previously" for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes.

An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For zero trust, client identity includes the user account and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state includes device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include automated user analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a user, data asset, or application. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. "Least privilege" principles are applied to restrict both visibility and accessibility.

5. The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.

No device is inherently trusted. Here, "most secure state possible" means that the device is in the most practicable secure state and still performs the actions required for the mission. An enterprise implementing a ZTA should establish a CDM or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Devices that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise, may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources.

6. All resource authentication and authorization is dynamic and strictly enforced before access is allowed.

This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multi-factor authentication (MFA) for access to some or all enterprise resources. Continuous monitoring with possible reauthentication and reauthorization occurs throughout user interaction, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous user activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.

7. The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

An enterprise should collect data about network traffic and access requests, which is then used to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

Zero Trust Design

In summary, zero trust is a shift away from wide network perimeters towards a narrower focus on protecting individual or small groups of resources where implicit trust is no longer granted to systems based on their physical or network location. In the zero trust framework (Figure 1), user privileges and access to data for zero trust must now be dynamic and strictly enforced before access is allowed and access to resources is determined by dynamic policy, based on behavioral attributes.

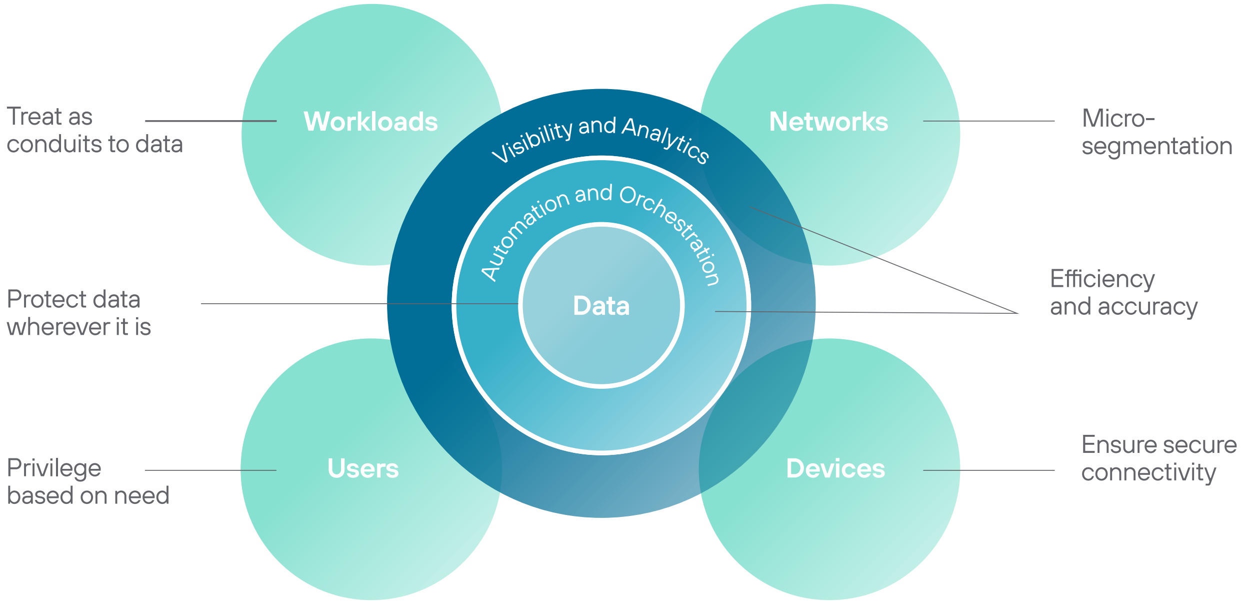
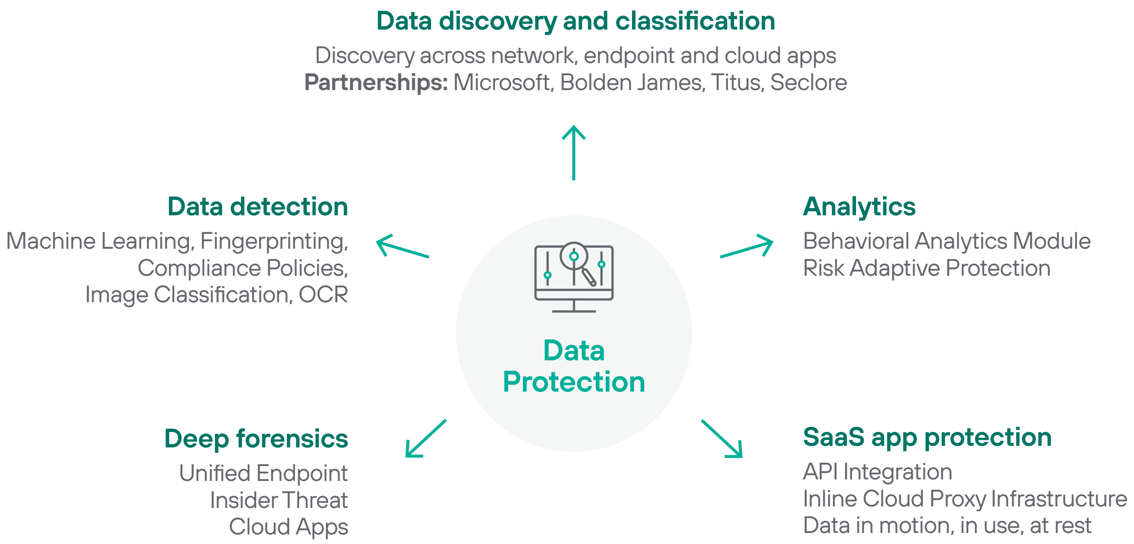


Figure 1: The zero trust framework

In the zero trust framework (Figure 1), users and their identities play a pivotal role, and organizations must ensure on a continuous basis that only authenticated and authorized users and devices can access applications and data. The easiest way to validate the identity of a user is through MFA.

Users Are at the Center of the Zero Trust Model

In the zero trust framework (Figure 1), data is at the center of the model for a reason. Protecting the data is a core component to zero trust security. Within zero trust, paying attention to who uses the data and what they do with it is what matters. Finding out what the users are doing and how they are accessing that data and securing it is the basis of a zero trust approach. A perimeter approach granted access based on implicit assumptions of trust. A zero trust approach must eliminate lateral movement and overly prescribed admin credentials to get to zero, then architect around that. With this approach, capabilities are limited to what is needed, therefore if a breach happens the problem is localized, and the size and scope of the breach will be less devastating. For this reason, data discovery and classification, data detection, deep forensics, analytics, and SaaS application protection are integral components of the zero trust model (Figure 2).



Data discovery and classification
Discovery across network, endpoint and cloud apps
Partnerships: Microsoft, Bolden James, Titus, Seclore

Data detection
Machine Learning, Fingerprinting,
Compliance Policies,
Image Classification, OCR

Analytics
Behavioral Analytics Module
Risk Adaptive Protection

Data Protection

Deep forensics
Unified Endpoint
Insider Threat
Cloud Apps

SaaS app protection
API Integration
Inline Cloud Proxy Infrastructure
Data in motion, in use, at rest

Figure 2: Data is at the center of a zero trust model

A Case for Thinking Beyond Identity

In the zero trust framework, users and their identities also play a pivotal role, and organizations must ensure on a continuous basis that only authenticated and authorized users and devices can access applications and data. The easiest way to validate the identity of a user is through multi-factor authentication.

Multi-factor authentication strengthens access security by requiring two or more factors to establish the identity. These factors can include something you know—like a username and password, something you have—like a smartphone app to approve authentication requests, or something you are—like a fingerprint.

MFA solutions have evolved to include user and device context. Contextual information like the user's device, the network used for access, or a geographic location can be used to compel users to provide additional factors to re-verify their identity.

However, just using the contextual background is still not enough when designing a zero trust environment! We have come across incident after incident where insiders with the right access have walked away with sensitive data. We can speculate that had zero trust tenets been in place, Edward Snowden would have been unable to obtain the broad range of documents that he released to the public. Instead, he was given "system administrator" privileges within the NSA network, which provided him blanket access to resources and files. Snowden may not have needed that access to perform his duties. But for someone who is in a role requiring system administrator privileges and access to do their job, how can we then ensure that when they access privileged information, it is solely to do their job and nothing else?

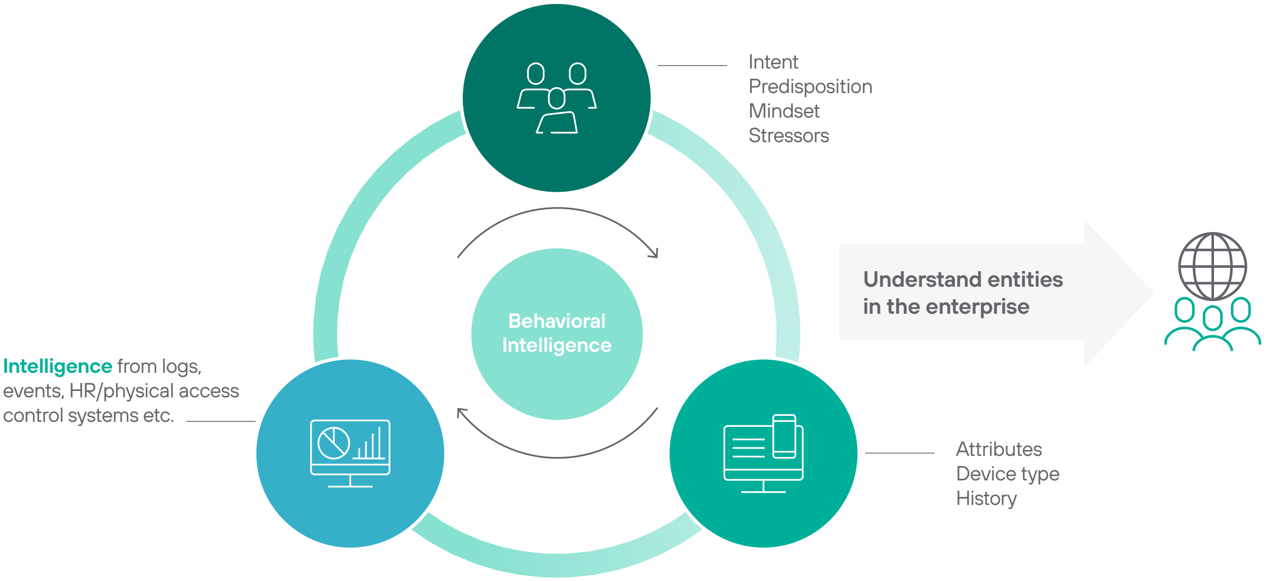
Understanding context can help, but it is critical to understand intent.

Forcepoint's approach to understanding intent

Forcepoint's behavioral intelligence not only looks at IT environmental data such as logs, events, HR databases, and physical access control systems, but also uses an understanding of human behavior—including intent, predisposition, and stressors, as well as device context—to identify risky users. With privacy in mind, the user data is anonymized, and the identities that deviate from normal behavioral patterns result in elevated risk scores for those user identities.

+ Understanding context can help, but it is critical to understand intent.

Figure 3: Behavioral Intelligence enhances understanding of risk users


Intent
Predisposition
Mindset
Stressors
Behavioral Intelligence
Understand entities in the enterprise
Intelligence from logs, events, HR/physical access control systems etc.
Attributes
Device type
History

Forcepoint Behavioral Analytics enables security teams to proactively monitor for high-risk behavior across the enterprise. Forcepoint security analytics platform provides unparalleled context by fusing structured and unstructured data to identify and disrupt malicious, compromised, and negligent users to help uncover critical problems such as compromised accounts, corporate espionage, intellectual property theft, and fraud.

Forcepoint Behavioral Analytics provides insight into high-risk behaviors and individuals, not just anomalous alerts. This more automated approach to security reduces the need for human intervention until an actual investigation is warranted, pseudonymizes user identity, and lessens the possibility for human error and bias. This method means that employees are treated fairly and equally, with access to data collected limited in visibility only to the required security teams. Dynamic, automated security empowers organizations to elevate their cybersecurity regime, while keeping privacy at the forefront. By evaluating nuanced interactions between people, data, devices, and applications, Forcepoint prioritizes timelines for security teams. Our software is built upon four pillars:

→ **Rich context.** Fuses disparate data sources into a single narrative, combining communications content to decipher intent alongside SIEM, endpoint, and employee enrichment feeds.

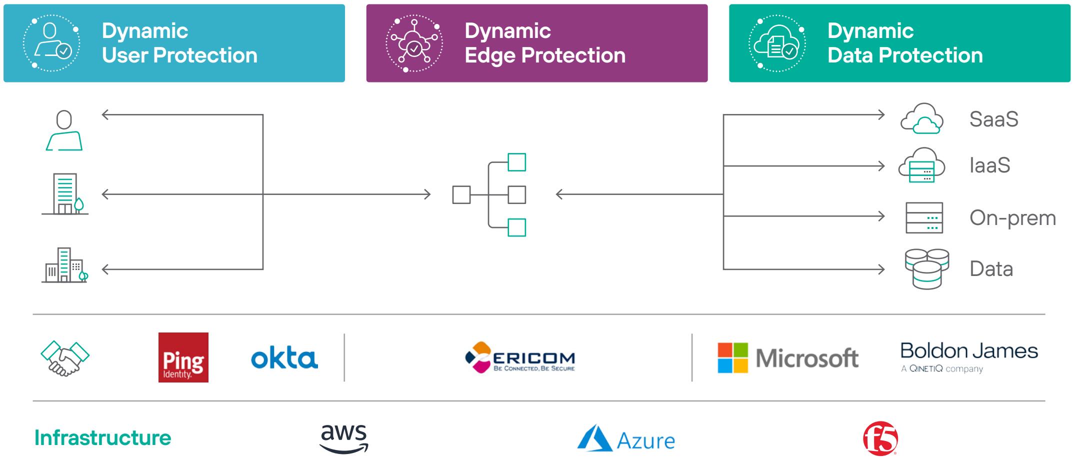
→ **Hybrid analytics.** Applies multiple types of rigorous behavioral and content-based analytics focused on change, pattern, and anomaly detection to better detect sophisticated attacks.

→ **Search and discovery.** Utilizes powerful forensic search and discovery tools through a context-rich user interface for ongoing monitoring and deep-dive investigations.

→ **Intuitive workflow.** Delivers proactive reporting that fully integrates with human workflows and existing client information architectures to streamline operational efficiency.

Forcepoint Zero Trust

Agencies moving toward zero trust will benefit from integrated security solutions that can adapt dynamically to risk and provide real-time reporting that generates actionable insights. Unlike point product vendors, Forcepoint offers a full and integrated security portfolio that helps agencies implement a practical approach to implementing zero trust (Figure 4).



I. Continuous user risk evolution by integrating user protection with IAM

II. Network micro-segmentation with edge protection

III. Secure connectivity with unified endpoint and RBI

IV. Cloud workload protection with AWS and Azure integration

V. Classify and protect data on-prem & in cloud with data protection

VI. Enable risk-adaptive response

Figure 4: Forcepoint practical approach to implementing zero trust

Comprehensive Web+Cloud protection

To safely harness cloud-based resources that will drive your agency forward, you need a comprehensive solution with controls for both users and data. Unlike competitors who focus on one specific product category, Forcepoint's solution combines various capabilities from Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), and Data Loss Prevention (DLP) products. With Forcepoint, you can secure:

→ Users, whether they're on-premises, on the road, or working remotely.

→ Data, both on-premises and in the cloud.

→ Access to cloud applications without hindering productivity.

Boundary control

As a leader in both cross-domain and network security technologies, Forcepoint is uniquely positioned to provide a sophisticated integration for extremely resilient architectures. Together, these technologies deliver a much sought-after, high-availability boundary control solution.

→ **Automate high-speed, secure transfer** of data between source and destination networks for critical infrastructure and multiple security domains.

→ **Protect networks from intrusion** with IDS, IPS, VPN tunnel encryption, SDWAN mobility, supporting network self healing.

→ **Automate network protection** failover with uniquely 16x scalable firewall clusters providing zero-downtime, hot swappable, and load-balancing network security.

Behavioral analytics

With an evolving threat landscape, your agency needs to be more proactive about threat management. Forcepoint is one of the only vendors to offer seamless integration with its Behavioral Analytics product to monitor for high-risk behavior and prevent data exfiltration from accidental, malicious, and compromised users, giving you:

→ **Comprehensive visibility** through examination of structured and unstructured business data and communications.

→ **Deep context** around behaviors that may indicate unwanted activity.

→ **Flexibility** to customize risk models to support any use case.

→ **Efficient investigations** with in-depth analytics.

.

Risk-adaptive protection

As one of the NIST tenets of a zero trust architecture states: "Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes." With less time to decipher disparate data, chase false positives, and manage exceptions, to achieve this you need dynamic security that adapts to real-time changes in risk. Only Forcepoint offers a risk-adaptive approach that leverages behavioral analytics, unified policies, and orchestration to rapidly identify risk, automate policies, and reduce the quantity of alerts requiring investigation, empowering you to:

→ **Capture interactions** between users and data everywhere.

→ **Generate** a dynamic risk score by understanding context.

→ **Respond automatically** to compromised, accidental, and malicious behavior.

→ **Gain efficiencies** in investigation and operations through context, such as detailed timelines of events.

Actionable insights

Chasing perceived threats is ineffective. You need a better understanding of where to start looking, whether it's to understand potential threats, possible compliance issues, or opportunities for better user productivity or operational efficiency. With Forcepoint, you'll get the actionable insights you need to determine:

- → From where in your organization data is moving out to the web and the cloud.
- → What external applications IT users are consuming, whether they are a risk, and a cause for underutilization of sanctioned applications.
- → Unusual patterns of behavior, possibly pointing to malicious intent or misunderstandings of published governance guidelines.
- → What types of applications users perceive they need to better do their job.

Forcepoint technology alliance ecosystem

Forcepoint user protection solutions can both directly ingest relevant context from identity and access management (IAM) solutions and (optionally) enrich them with risk user information to dynamically enforce policies.

Two IAM/IDaaS ecosystem partners that integrate with Forcepoint's Behavioral Analytics and are now available for use are Okta and Ping. The combined solution delivers enriched visibility into user activities, enhances risk scoring, and enables risk adaptive authentication policy for joint customers. Forcepoint plans to continue to add technology alliance partners to its ecosystem. We plan to enable customers to drive risk-adaptive authorization to key enterprise resources such as critical data. Stay tuned for exciting developments in this area.

+ Learn more about Forcepoint solutions at forcepoint.com

About the Author

Jill Bradshaw is a Senior Product Marketing Manager with Forcepoint's Global Government & Critical Infrastructure team. She has more than 15 years of experience in the technology industry with a focus on security and networks, the majority of that time focusing on solutions for global government customers.

Jill holds a MBA from Baylor University and received her BA from Texas Tech University. When not thinking about security technology, she enjoys camping and spending time with family and serves on the leadership teams for the Texas Chargers and Protect Texas Fragile Kids organizations.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.