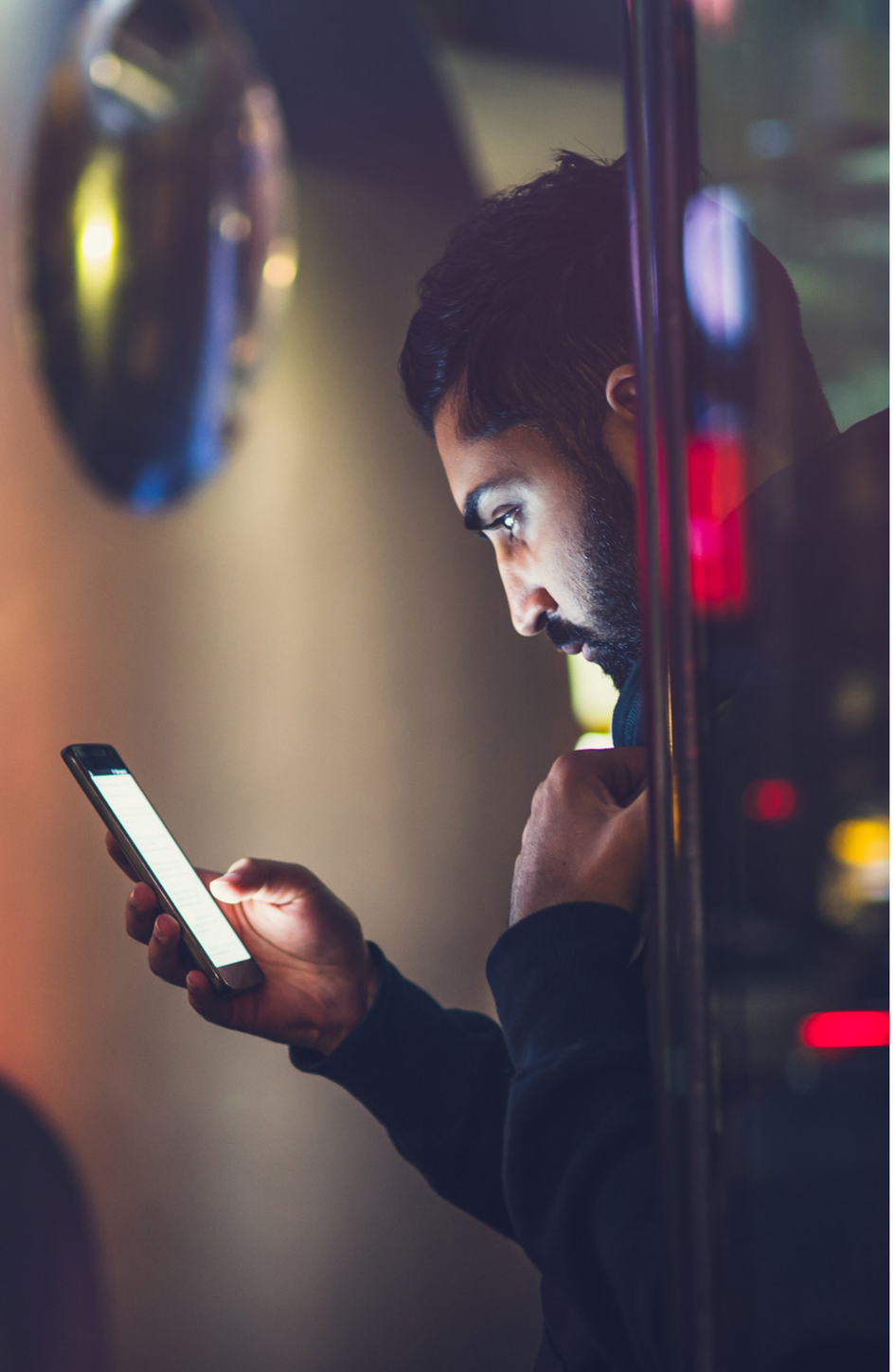
Enterprise Strategy Group | Getting to the bigger truth.™

A Strategic Approach to Zero Trust Security

The Spectra Alliance

By Carla Roncato, Senior Analyst; and Dave Gruber, Senior Analyst

JULY 2021



CONTENTS

What is Zero Trust?

Zero trust (ZT) is a strategy for improving an organization's security posture by focusing on protecting resources such as identities, data, and applications while minimizing the attack surface and access to development environments, corporate networks, and infrastructure. Zero trust is not a product, but rather a formula or model that assumes there are no perimeters, no safe zones, no safe users, and, therefore, zero trust.

While familiarity with zero trust is relatively high among organizations, a recent ESG research survey uncovered that definitions vary among organizations and most organizations began without a zero trust strategy.[1]

Figure 1. Organizations' History with Zero Trust

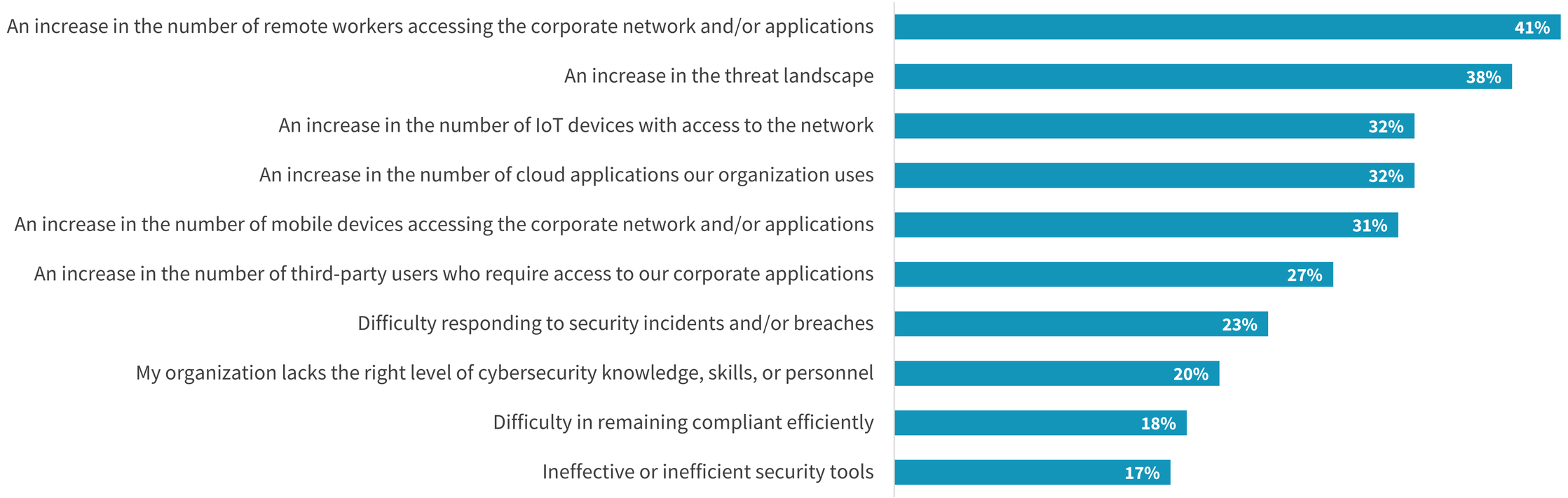
Question text: Which of the following statements best describes your organization's history with zero-trust?
(Percent of respondents, N=375, multiple responses accepted)

[1]Source: ESG Research Report, *The State of Zero Trust Security Strategies*, April 2021.

Back to Contents

As modern security organizations continue to make zero trust a core strategy, most find it increasingly difficult because they face expanding access needs and increasing threat landscape,[2] so they struggle with which approach is right for them and where to start.

Figure 2. Reasons that Cybersecurity Has Become More Difficult



Question text: In your opinion, which of the following factors have been most responsible for making cybersecurity management and operations more difficult? (Percent of respondents, N=249, three responses accepted)

This paper is a practical guide to zero trust that explores the factors that organizations should consider, the approaches and options available, different ways of scoping projects across the six elements of zero trust, and recommendations to begin the journey.

[2]Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2021.

Back to Contents

Why is Zero Trust Important?

Digital transformation initiatives, the increase in the ability for employees to work from anywhere, and the pervasiveness of security threats have resulted in the rise of the concept of zero trust, which is a significant departure from traditional network security and "trusted network" architectures.

The ability to work from anywhere creates a need to support hybrid use cases, which include secure access to data, tools, resources, and systems from a multitude of on-premises, private, and public cloud infrastructures, in addition to a plethora of software-as-a-service (SaaS) applications.

Enabling flexible, anywhere, and anytime scenarios is driving many organizations to re-evaluate both their operating model and security model to consider one that is based around both productivity and security, while recognizing it results in an extended attack surface in a more complex threat landscape.

Least-privilege access has been a security philosophy for many years. However, zero trust takes least-privilege access to a new level, by involving identities, devices, data, applications, and a network architecture that moves security controls to contain the attack surface and minimize catastrophic impact to business operations.

As a relatively new company, we are cloud focused overall and so is our approach to zero trust security. I think of it from a service standpoint, which service am I standing up and the zero trust principles around it--core for us is cloud identity and security controls."

- David W, Director of IT, Technology Vendor in Logistics Industry

Back to Contents

Is Zero Trust Right for Your Organization?

While zero trust is a broad initiative, there are a few factors for organizations to consider that are especially well suited to zero trust. If any combination of these factors and considerations resonates now or as part of a digital transformation initiative, then a Zero Trust security model will likely benefit your organization.

1. DOES YOUR ORGANIZATION HAVE A HIGHLY DISTRIBUTED WORKFORCE AND DEVICE ECOSYSTEM, SUCH AS IN THE FOLLOWING SITUATIONS?

- Modern organizations with business operations that encompass a combination of employees, partners, contractors, vendors, and other third-party service providers.
- Employees that require special access to restricted applications, mission-critical systems, and regulated and sensitive data from a variety of managed and unmanaged endpoints and devices.
- Security mechanisms that no longer support the organization's modern operating model, such as the traditional use of virtual private networks (VPNs) and password-based authentication.
- Devices and endpoints that may or may not be managed by your organization that run various operating systems and software to enable employees to conduct business and collaborate.

---

2. DO YOU HAVE A MULTI-GENERATIONAL, HYBRID OPERATING ENVIRONMENT, SUCH AS IN THE FOLLOWING SITUATIONS?

- Diverse mixture of data center technologies, cloud infrastructure providers, platforms and application stacks with varying asset, management, and maintenance lifecycles.
- Application development environments for modernizing or creating new applications, products, and services used by developers, testers, engineers, and operations teams or creating new ones.
- Challenges with visibility into the users, accounts, resources, and machines across your extended environment and the levels and types of permissions that exist, as well as the risks they may pose.
- Inconsistencies in configurations, integrations, controls, patching, and protection coverage due to complexity, velocity, skills, expertise, or inadequate solutions.

---

3. DO YOU HAVE A BROAD DATA MANAGEMENT LANDSCAPE AND DATA OWNERSHIP, SUCH AS IN THE FOLLOWING SITUATIONS?

- Private, sensitive, and regulated data storage (at rest) across your environments that requires consistent data encryption and protection that meet audit and compliance mandates.
- Data creation, collection, collaboration, and monetization activities across your environments that require continuous discovery, integration, classification, and preparation for business use.
- Big data platforms, DataOps, and AI/ML model development for use in a variety of business intelligence and analytical applications by data engineers, data scientists and data analysts.
- Challenges with governing access across data users, owners, stewards, and processors, as well as managing the the data lifecycle and data movement, and the risks they may pose.

Back to Contents

Approaches to Zero Trust

Like so many security frameworks of the past, virtually every security vendor has a zero trust story. We have broken down four approaches and provided guidelines for how to think about your strategy and choose the right zero trust approach for your organization and goals:

DIVERSIFIED

A diversified approach is one that enables organizations who already have strong security practitioners and well-established security operations to select technologies from a diverse set of vendors to achieve a desired zero trust security model. It considers that the organization already has a zero trust journey mapped out across the six elements and that internal teams are leading the execution aligned to their operating model, technology investments, business priorities, and outcomes.

CONSOLIDATED

A consolidated approach is one in which an organization intends to rely on one primary security platform vendor for most of their zero trust strategy. In some cases, this might be a cloud services provider that also supports the majority of zero trust elements or a pure-play security vendor that is deeply integrated and consolidated around a hyperscaler platform and roadmap. It considers that an organization is predominantly seeking cloud-native and cloud-centric security as its operating model, even if all elements of zero trust are not (yet) available.

STRATEGIC

A strategic approach is one that provides organizations with zero trust advisory, technology, and support across the breadth of six elements, agnostic of deployment model and cloud providers. It considers that organizations have depth of need in two or more areas of zero trust, such as identity, devices, and data; or applications, networks, and infrastructure. These organizations can extend and expand their existing investments with strategic platforms to achieve a zero trust security model.

MANAGED

A managed security services provider (MSSP) is another approach that relies on outsourcing to provide an organization with a mechanism to achieve a zero trust security model. MSSPs vary in their scope, coverage, products, and service levels. Therefore, it is incumbent upon the organization to assess if the zero trust service offerings align with and scale to their business, operating model, and security strategy.

Back to Contents

Choosing the Right Approach to Zero Trust

A DIVERSIFIED APPROACH IS BEST SUITED FOR ORGANIZATIONS WITH:

- √ A strong security program and practitioners.
- √ A well-established security operations center (SOC).
- √ Alignment on zero trust architecture.
- √ A prioritized zero trust journey map/plan.
- √ The ability to manage/maintain many tools.
- √ Varied licensing and pricing requirements.

A CONSOLIDATED APPROACH IS BEST SUITED FOR ORGANIZATIONS WITH:

- √ Significant investments in a primary security platform vendor.
- √ Deep integrations with a cloud services provider.
- √ Alignment on zero trust strategy and roadmap.
- √ A cloud-native/centric security operating model.
- √ Acceptable gaps in elements of zero trust
- √ Preference for usage and subscription-based bundles.

A STRATEGIC APPROACH IS BEST SUITED FOR ORGANIZATIONS WITH:

- √ Advisory, technology, and support services requirements.
- √ No preference in choice of deployment model and cloud providers.
- √ Depth of need in two or more elements of zero trust.
- √ Existing investments with strategic platform vendors and roadmaps.
- √ Interoperability and automation across platforms for visibility.
- √ Orientation around outcome-based KPIs and flexible contracting agreements.

A MANAGED APPROACH IS BEST SUITED FOR ORGANIZATIONS THAT:

- √ Have limited internal expertise in security technologies and zero trust strategies.
- √ Need for coverage to be aligned with business location/regions.
- √ Want vendor management capabilities for oversight and governance.
- √ Will benefit from service offerings tailored to industry-specific requirements.
- √ Prefer long-term service agreements.
- √ Desire fixed-price, multi-year agreements based on service level.

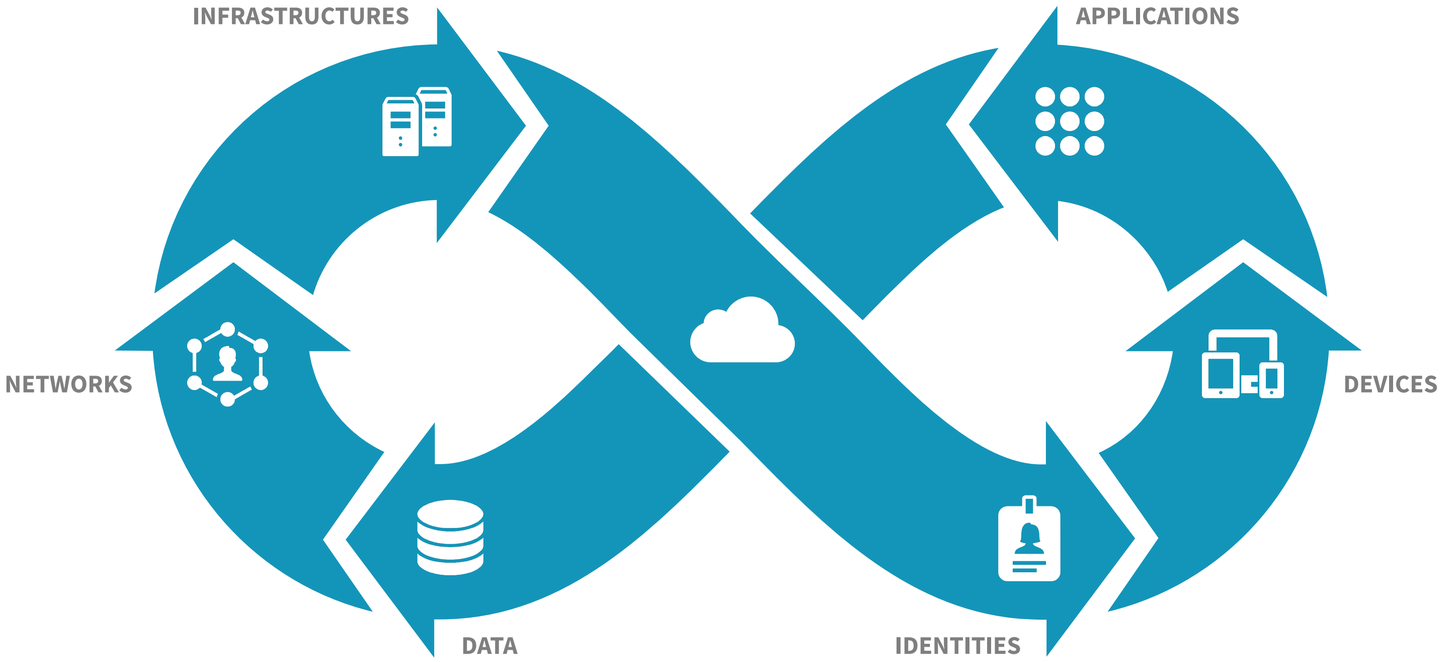
Back to Contents

Introducing the Spectra Alliance, a Strategic Approach

The Spectra Alliance helps organizations accelerate their journeys to zero trust. Current Spectra Alliance members include:

- **CrowdStrike**, providing endpoint security, cloud security, security operations, threat intelligence, and identity threat protection.
- **Netskope**, providing web gateway, cloud access security broker, and zero trust.
- **Okta**, providing cloud workforce identity, cloud customer identity, access management, and adaptive multi-factor authentication.
- **Proofpoint**, providing email security, cloud access security broker, data loss prevention, and secure access service edge.

Figure 3. Spectra Alliance



CROWDSTRIKE

- Endpoint and Cloud Security
- Security Operations
- Threat Intelligence
- Identity Threat Protection

netskope

- Secure Access Service Edge
- Cloud Access Security Broker
- Data and Threat Protection
- Zero Trust Network Access

okta

- Cloud Workforce Identity
- Cloud Customer Identity
- Access Management
- Adaptive MFA

proofpoint.

- Email Security
- Cloud Access Security Broker
- Data Loss Prevention
- Secure Access Service Edge

Back to Contents

To facilitate zero trust, we have built relationships—with audit, finance, legal and across IT and we have fantastic support from our executive leadership and board of directors. We use this same approach with our security vendors, and it is a key reason that our zero trust security strategy is where it needs to be. **We have a culture of do the right thing by our people and take risk management seriously.**

- *John B, Enterprise Security Manager, US Manufacturer in Construction Industry*

THE ALLIANCE STRIVES TO HELP ORGANIZATIONS:

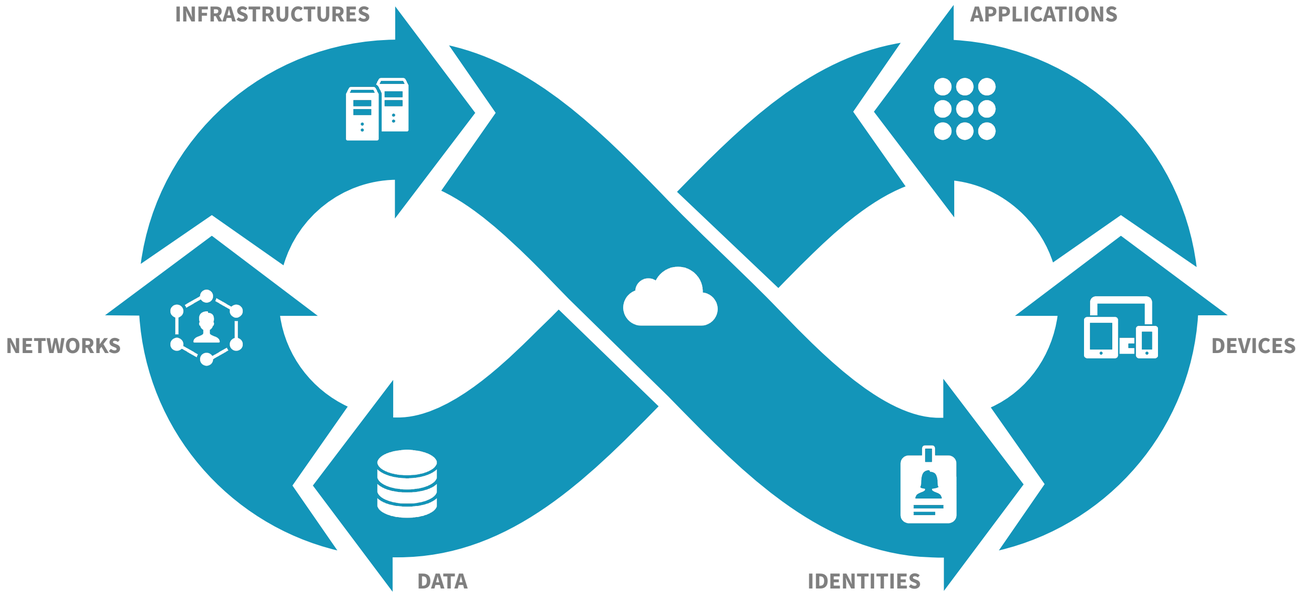
- **Increase Coverage:** The alliance works for both distributed and office scenarios with no rip-and-replace requirements, regardless of which devices, users, networks, and applications are used or where they are located.
- **Reduce Risk:** The alliance protects against modern and evolving threats against multiple attack vectors, securing all hardware (laptops, mobile phones, servers, and IoT devices) and digital assets (user accounts, certificates, applications, and data).
- **Move to an Interoperable Architecture:** The alliance helps organizations to achieve a zero trust architecture with best-of-breed cybersecurity vendors leveraging plug-and-play integrations, allowing them to future-proof their investments.
- **Deploy Frictionlessly:** With pre-integration across the journey to Zero Trust, the alliance helps organizations drive down complexity and risk exposure.
- **Operate Cost-efficiently:** Across both CapEx and OpEx, the alliance helps organizations to streamline their resources, staff, and longer-term operations and minimize unknown financial considerations.

Back to Contents

Elements of Zero Trust

Scoping zero trust involves six elements: identities, devices, applications, data, networks, and infrastructure. All six elements are not mandatory (some elements may have more merit than others), and not all use cases and techniques are explored. Some elements may not require new tools but rather a change in processes or policies to achieve zero trust outcomes.

These are some common use cases that enable zero trust.



Identities: Supporting techniques include multi-factor authentication, least-privilege/adaptive access, explicit and continuous verification, lateral movement controls for service accounts, and usage/behavioral monitoring.

Devices: Supporting techniques include un/managed devices, asset discovery, device characteristics (type, location, purpose, version), device health, usage patterns, and behavioral monitoring.

Applications: Supporting techniques include modern API and in-app permissions, real-time inspection, app risk scoring and monitoring, secure configuration validation, app leakage (data, code).

Data: Supporting techniques include automated discovery, classification, labelling, encryption, least-privilege data access, privacy-enhanced/minimal collection, monitoring.

Networks: Supporting techniques include micro-segmentation, end-to-end encryption, intrusion/threat detection and response, network monitoring, activity visibility, and analytics.

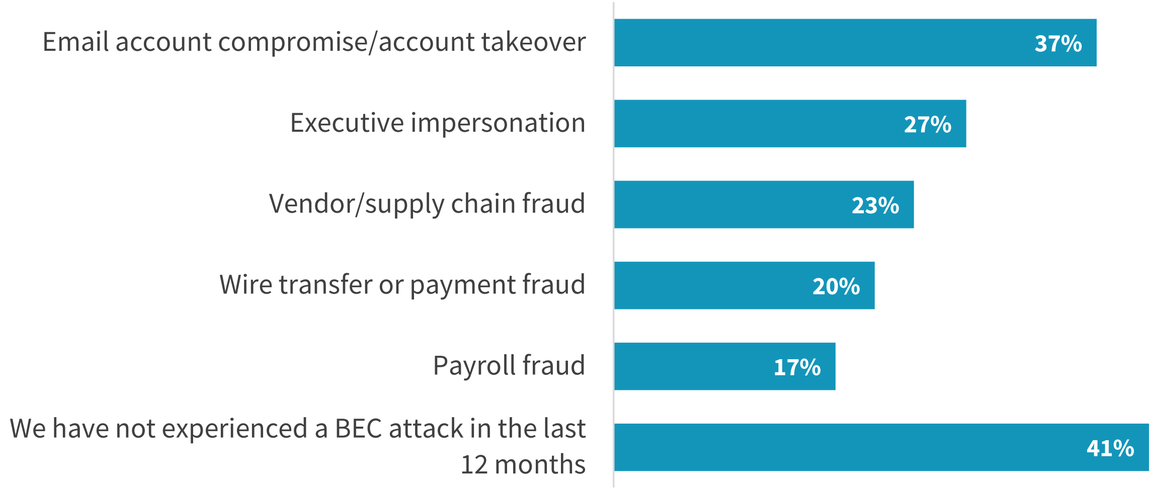
Infrastructures: Supporting techniques include VMs, containers, orchestration, microservices, configurations, versioning, patching, activity visibility, and monitoring.

Back to Contents

Identities as a Starting Point

Due to high rates of compromised credentials as a root cause of data breaches and malicious activity, identity-related attacks represent a significant risk to organizations. The most prevalent technique is phishing, where attackers send malicious emails and fake login forms designed to trick people to reveal credential information such as usernames and passwords, as well as other sensitive and financial information. Additionally, email accounts are often used as a mechanism to receive password reset links and account alerts, which make them valuable to attackers in personal and professional scenarios. According to ESG research, 6 in 10 organizations reported experiencing a business email compromise (BEC) attack.[3]

Figure 4. Organizations' History with Zero Trust



Question text: What types of business email compromise (BEC) attacks has your organization experienced within the last 12 months? (Percent of respondents, N=403, multiple responses accepted)

SPOTLIGHT ON PROOFPOINT: Proofpoint Email and Cloud Security

Proofpoint Email and Cloud Security

Proofpoint protects against business email compromise (BEC) by addressing the many tactics used by threat actors. Tackling the problem in this way prevents threats that use display name spoofing, domain spoofing, and look-alike domains. It also helps to prevent these threats from impacting partners and customers with DMARC email authentication.

Proofpoint Cloud Access Security Broker protects against the propensity of credential reuse across different cloud application accounts that an end-user might have, including both personal and corporate accounts. With visibility and control across cloud applications, email, and personal webmail, organizations can implement a zero trust approach to help prevent the loss of credentials and identify suspicious behavior accessing these accounts. It is critical to be able to identify attempted cloud account compromise and the symptoms of accounts that are already compromised.

Spectra Integrations: Proofpoint and CrowdStrike integration delivers best-of-breed threat intelligence sharing and analysis. Together, Proofpoint and Okta make security orchestration faster and easier by integrating best-of-breed solutions to provide accurate, timely response to credential phishing attacks.

[3]Source: ESG Research Report, *Trends in Email Security,* August 2020.

Back to Contents

While phishing is one of the easier social engineering techniques that attackers use, it is not the only one. According to Verizon's 2021 Data Breach Investigations Report:[4]

89%
of web application breaches were caused by credential abuse.

36%
of breaches stemmed from phishing.

61%
of all breaches involved stolen credentials.

As a result of these attack techniques, zero trust is driving a focus on identity security and verification. Organizations that start their zero trust journey with identities typically begin by employing multi-factor authentication (MFA) to go beyond a single password by eliminating them entirely and/or adding two or more factors of proof on the authenticity of the user.

MFA can, or can be perceived to, create friction for end-users. To combat this friction, many organizations are including device characteristics and device health as a condition for context-based access decisions, which are silent to the end-user.

SPOTLIGHT ON OKTA: Identity Assurance – Never Trust, Always Verify

Okta Workforce Identity

Cloud-to-ground protection: Okta secures accounts, apps, servers, and resources and provides a network effect, automatically blocking suspicious IP addresses that have attempted identity attacks on other organizations with Okta ThreatInsight.

Use Factors that Balance Users and Security: Okta Adaptive Multi-Factor Authentication (AMFA) determines when to prompt for step-up authentication prior to granting access based on device and user context. Prompts are dynamic, based on user and device context to prevent overburdening the end-user.

Add Context to Policies: Okta is all about visibility into an organization's data and control over the policies that permit access. With more context around users, organizations can layer protection based on suspicious behaviors compared with their team's day-to-day behaviors.

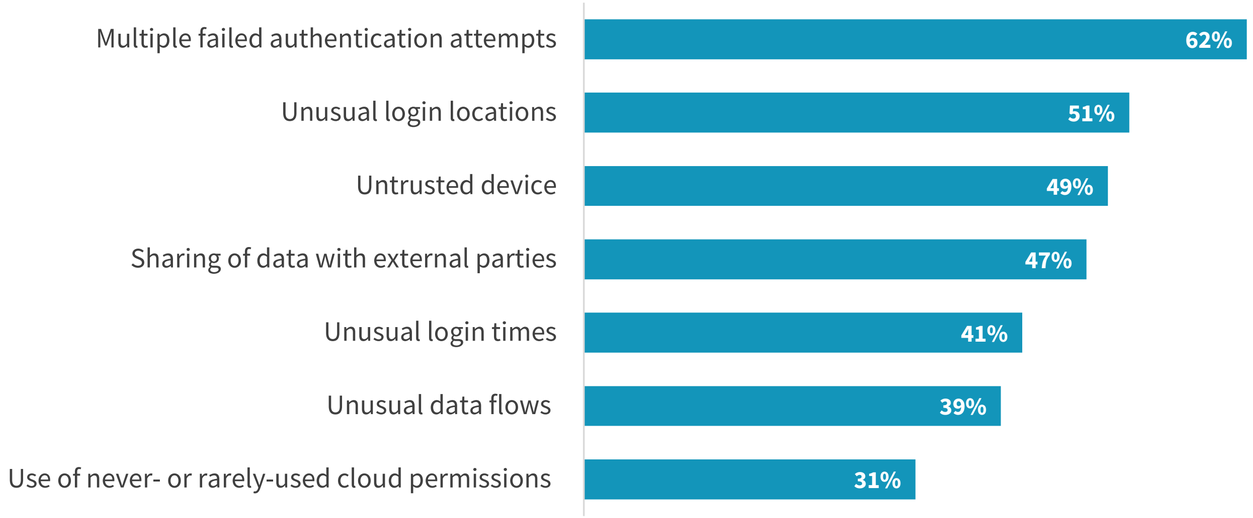
Spectra Integrations: Centralized, real-time reporting of all authentication events also enables organizations to investigate red-flag events and integrate with their other alliance member security tools. Okta's API provides AMFA logs of who is signing in to what, when, and where. Netskope integration enables step-up authentication based on adaptive policy controls, and CrowdStrike integrations enables real-time identity-related threat protection.

[4]Source: Verizon, *2021 Data Breach Investigations Report.*

Back to Contents

Visibility into identity-related behavior, privilege escalation, usage, attacks, and anomalies is a critical requirement for any zero trust identity project. User monitoring is also essential when it comes to use of cloud applications and services. Recent ESG research findings uncovered that 62% of organizations use or plan to use multiple failed authentication attempts as an indicator of account takeover (ATO), followed by 51% that will look for unusual log-in location characteristics, and 49% that will monitor untrusted/unknown devices as indicators.[5]

Figure 5. User Cloud Application and Services Actions to be Monitored for Threat Detection and Response Purposes



Question text: Which of the following user actions related to access to and use of your organization's cloud applications and services do you currently use, or plan to use, to monitor for threat detection and response purposes? (Percent of respondents, N=379, multiple responses accepted)

SPOTLIGHT ON CROWDSTRIKE: Identity Threat Protection

CrowdStrike Falcon Identity Threat Protection (ITD)

Secure Active Directories: CrowdStrike Falcon ITD improves AD security hygiene with continuous monitoring for credential weakness, access deviations, and password compromises, providing dynamic risk scores for every user and service account.

Monitor Access Activity reduces the attack surface by identifying over-permissioned admins, misused service accounts, and anomalous user behavior in virtual desktop infrastructure (VDI), remote-desktop attempts, and insider lateral movement and elevation of privilege requests.

Spectra Integrations: Pre-integrations with Okta AMFA and OKTA Single Sign-On and available APIs enable real-time, identity-related threat protection. Proofpoint and CrowdStrike integration delivers threat intelligence sharing and analysis. Netskope and CrowdStrike integrate on EDR, threat detection and response, and intelligence exchange.

[5]Source: ESG Research Report, *Trends in Identity and Access Management: The Increasingly Cloud-driven Identity Landscape,* February 2021.

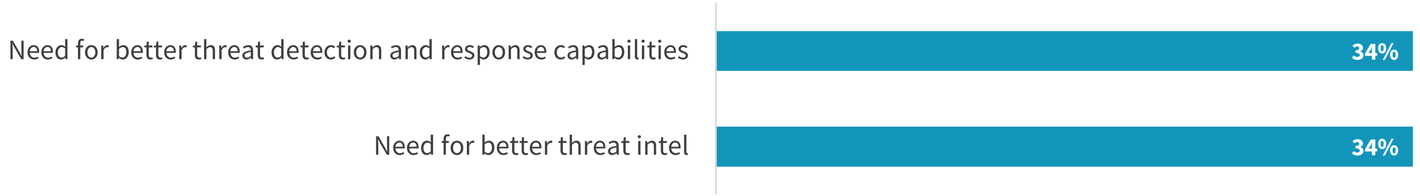
Back to Contents

Devices as a Starting Point

Endpoints are the most common entry point for initial compromise. Among various available entry points, including email payloads, phishing-driven domain spoofing, and external device malware, endpoint attacks are the frontline for attack entry. When endpoint devices become compromised, attackers often attempt to move laterally to other devices for reconnaissance and ultimately to breach information. When endpoint security controls can warn network and cloud security edge services and identity and access management (IAM) controls of potential compromise, both inbound and outbound lateral movement can be stopped.

Organizations should strongly consider on all public-facing employee services and portals, adding an additional layer of access control from all devices. In addition to MFA, a robust privilege access management process can limit the damage adversaries can do if they get in, while further reducing the likelihood of lateral movement. Because sensitive data often resides on endpoint devices, accurate data classification and sensitive data encryption can limit exposure from compromised endpoints. When data protection controls work together with endpoint controls, access is limited to authorized users. Compartmentalizing and restricting data access reduce potential damage from unauthorized access to sensitive information. Adding identity security helps protect against intrusions from compromised credentials or vendor/contractor endpoints lacking the same coverage.

Figure 6. Top Two Reasons for Switching Endpoint Security Vendors[6]



Question text: If your organization recently switched or has an active project to switch endpoint security vendors, what drove/is driving this change? (Percent of respondents, N=271, multiple responses accepted)

SPOTLIGHT ON CROWDSTRIKE: Endpoint Security

CrowdStrike Falcon Endpoint Security and Device Control

The CrowdStrike Falcon cloud-scale platform analyzes incoming real-time data on a massive scale, crowdsourcing upward of 1 trillion endpoint-related events per day as they occur across the global CrowdStrike community. This stream of real-time threat information drives the proprietary AI-powered CrowdStrike Threat Graph® database, dynamically scrutinizing event-based data to detect anomalous behavior based on indicators of attack (IoAs) in addition to IoCs. CrowdStrike provides customers with protection and visibility across the entire threat lifecycle, no matter where the endpoints and workloads are located.

Unlike systems that rely solely on IOCs, which appear only after a breach has already occurred, IOAs are effective regardless of whether malware is present. This allows customers to detect and prevent attacks while they are still in progress and before data is exfiltrated.

Spectra Integrations: Integrations with Proofpoint deliver threat intelligence sharing and analysis; with Netskope on threat detection and response, and threat intelligence exchange; and with Okta for dynamic device posture assessment from devices that do not meet the posture requirements.

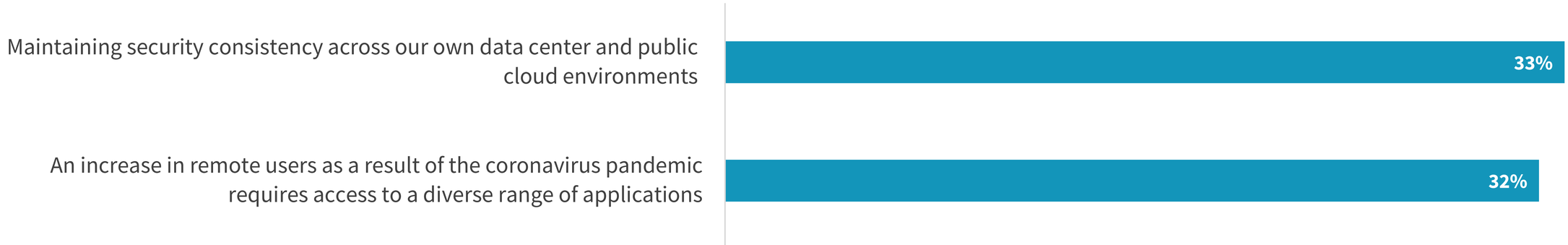
[6]Source: ESG Master Survey Results, *Trends in Endpoint Security*, March 2020.

Back to Contents

Applications as a Starting Point

In a work-from-anywhere world, user to application connectivity can include public cloud, private cloud, on-premises and SaaS applications, or more likely, a combination of all. Implementing consistent security policies across this array of applications requires a broad security mechanism, available to all users, regardless of their location. CASB inline and API inspection governs access and usage based on identity, service, activity, application, and data. Policies can be defined based on service category or risk, offering security controls such as block, alert, bypass, encrypt, quarantine, and coach for policy enforcement.

Figure 7. Top 2 Identity and Access Management Challenges Related to Cloud Services[7]



Question text: Which of the following represents the biggest identity and access management challenges created by your organization's use of cloud services? (Percent of respondents, N=379, three responses accepted)

[7]Source: ESG Research Report, *Trends in Identity and Access Management: The Increasingly Cloud-driven Identity Landscape,* February 2021.

Back to Contents

SPOTLIGHT ON NETSKOPE: Next Gen SWG

Netskope Next Gen Secure Web Gateway (SWG)

Govern Usage: For web access, managed SaaS, thousands of Shadow IT apps, public cloud services and public-facing custom apps inline. App risk ratings cover 28,000+ apps and cloud services, plus adaptive policy controls provide real-time coaching of users based on content and context, including data sensitivity, activity, and app instance.

Secure Data: Control unintentional and unapproved data movement, including between company and personal app instances. Data protection includes a wide range of app activity controls, standard DLP controls, plus advanced DLP including AI/ML classifiers for documents and images inline. Advanced analytics visualize data movement and risks across all user traffic including web, apps, and cloud services.

Protect Against Threats: Inspect TLS-encrypted inline traffic for web, apps, and cloud services for malware, plus web and cloud-enabled threats. Defenses include anti-malware engines, heuristics and pre-execution analysis, multiple sandboxes, ML analysis, remote browser isolation and intrusion prevention of client exploits.

Spectra Integrations: Netskope Cloud Exchange enables threat intelligence sharing with other defenses and ticket orchestration with SOAR and IR platforms. Netskope and CrowdStrike integrations support threat detection and response across endpoints and in the cloud, and threat intelligence exchange.

SPOTLIGHT ON PROOFPOINT: CASB

Proofpoint Cloud App Security Broker (CASB)

Proofpoint CASB combines compromised account detection, data loss prevention (DLP), cloud and third-party apps governance with adaptive access controls to help you secure your cloud infrastructure.

Contain Shadow IT: Proofpoint CASB analyzes your log files to discover your cloud services to assess their risk by using a catalog of 46,000 applications, with more than 50 attributes for each. It will determines vendor credibility, assesses vulnerabilities, and uncovers any security and compliance gaps to help contain shadow IT.

Protect Against Threats: Many third-party apps add more features to Microsoft 365, Google Workspace, Box and other platforms. But some are poorly built or overtly malicious. With Proofpoint CASB, you can discover, assess and control third-party add-ons, including the malicious ones. And with our powerful analytics, you can grant the right levels of access to these third-party, add-on apps based on the risk factors that matter to you.

Spectra Integrations: Proofpoint and CrowdStrike integration delivers best-of-breed threat intelligence sharing and analysis. Together, Proofpoint and Okta make security orchestration faster and easier by integrating best-of-breed solutions to provide accurate, timely response to credential phishing attacks.

Back to Contents

Data as a Starting Point

Data is everywhere. Managing data security consistency and compliance across on-premises environments is already challenging, and managing data security consistency in cloud environments can be substantially more challenging due to the distributed nature of applications, collaboration tools, and data platforms.

Recent ESG research found that more organizations prioritized data classification and security as the starting point for zero trust than any other security capability. Specifically, 41% view data classification and security as a starting point, and for 37% of organizations it is a secondary consideration.[8]

Figure 8. Importance of data classification and security for driving zero trust initiatives.[9]

Question text: To support zero-trust, how has your organization prioritized – or will it prioritize – implementing data classification and security capabilities? (Percent of respondents, N=421)

[8]Source: ESG Brief, *Re-emphasizing Data Security as Part of a Zero Trust Approach,* May 2021. [9]Source: ESG Research Report, *The State of Zero Trust Security Strategies,* April 2021.

Back to Contents

SPOTLIGHT ON NETSKOPE: Data Loss Prevention

Netskope Advanced Data Loss Prevention (ADLP)

Netskope 4-in-1 Data Loss Prevention for IaaS, SaaS, web, and email enables visibility into data everywhere it goes. It discovers cloud apps and then finds, classifies, and protects data used by these applications, as well as data moving within and between SaaS, IaaS, email, and web apps. Using advanced machine-learning-based data scanning and classification, DLP operations are automated and expedited.

Monitor and Detect Data Activity: Netskope ADLP can help organizations prevent the transferring, copying, downloading, uploading, viewing, and sharing of sensitive data to personal email accounts, personal devices, applications, social media, and personal cloud storage.

Spectra Integrations: Pre-integrations with CrowdStrike enable threat detection and response, plus threat intelligence exchange. Integration with Okta enables federation of SSO/MFA to managed and unmanaged apps, plus the ability to invoke step-up authentication based on adaptive policy controls.

SPOTLIGHT ON PROOFPOINT: DLP

Proofpoint DLP and Information Protection

Proofpoint DLP/Information Protection protects against data loss posed by negligent, compromised, and malicious insiders by aggregating content, threat, and user-behavior telemetry across channels in a unified alert and investigations interface to help organizations respond quickly to data risk.

Make Faster Decisions: With our people-centric approach, one can achieve a faster response and investigation time. The unified incident and investigations interface enables your security and compliance teams to respond quickly. Since visibility anchors on the person, you can shut down compromised cloud accounts or apply encryption to the email that triggered the policy.

Modern DLP Architecture: Scale and rapidly deploy sensors based on your organization and use cases. Achieve data residency requirements across the US and Europe. Achieve GDPR and privacy by design through industry-leading, attribute-based access controls.

Spectra Integrations: Proofpoint and CrowdStrike integration delivers best-of-breed threat intelligence sharing and analysis. Together, Proofpoint and Okta make security orchestration faster and easier by integrating best-of-breed solutions to provide accurate, timely response to credential phishing attacks.

Back to Contents

Networks as a Starting Point

Secure access service edge (SASE) can identify users and devices, apply policy-based security controls, and deliver secure access to the appropriate applications, cloud services, data, or websites. SASE makes it possible to provide secure access regardless of where users, data, applications, and devices are located.

Figure 9. Top Attribute in a SASE Implementation is an Ability to Scale[10]

ALL ORGANIZATIONS	EXTENSIVE CLOUD USERS	MORE THAN 100 BRANCH OFFICES	MORE THAN 25% ROAMING USERS
1. Ability to scale	**1. Ability to scale**	**1. Ability to scale**	**1. Ability to scale**
2. Int. w/ endpoint agents	**2. Hybrid options**	**2. Flexible pricing**	**2. Partner integrations**
3. Int. w/ on-prem DLP	**3. Int. w/ endpoint agents**	**3. Int. w/ endpoint agents**	**3. Hybrid options**
4. Hybrid options	4. Flexible pricing	4. Hybrid options	**3. Int. w/ endpoint agents**
5. Partner integrations	5. Int. w/ on-prem DLP	5. Partner integrations	5. Flexible pricing
6. Flexible pricing	6. Partner integrations	6. Int. w/ on-prem DLP	6. PoPs/Peering
7. Unified policy mgmt	**7. Unified policy mgmt**	**7. Unified policy mgmt.**	**7. Unmanaged devices**
8. Full proxy	**8. Full proxy**	**8. Unmanaged devices**	**8. Full proxy**
8. Unmanaged devices	**9. Unmanaged devices**	**9. Full proxy**	**9. Unified policy mgmt**
10. PoPs/Peering	10. PoPs/Peering	10. PoPs/Peering	10. Int. w/ on-prem DLP

[10]Source: ESG Research Report, *Transitioning Network Security Controls to the Cloud: The Emergence of Elastic Cloud Gateways*, August 2020.

Back to Contents

SPOTLIGHT ON NETSKOPE: SASE

Netskope Approach to SASE

Netskope provides cloud-native microservices in a single platform architecture that spans use cases, such as the ability to inspect SSL/TLS-encrypted traffic; decoding cloud and web traffic through an inline proxy (NextGen SWG); data, threat and intrusion protection for all ports and protocols (FWaaS); and integration with a software-defined perimeter (SD-WAN).

Done properly, a SASE eliminates perimeter-based appliances and legacy solutions. Instead of delivering the traffic to an appliance for security, users connect to the SASE cloud service to safely access applications, cloud services, data and websites with the consistent enforcement of security policy.

Spectra Integrations: Pre-integrations with CrowdStrike enable threat detection and response, plus threat intelligence exchange. Integration with Okta enables federation of SSO/MFA to managed and unmanaged apps, plus the ability to invoke step-up authentication based on adaptive policy controls.

SPOTLIGHT ON PROOFPOINT - SASE

Proofpoint's Approach to SASE:

Proofpoint provides a powerful, cloud-native platform aligned to the security industry's vision of SASE architecture, in which organizations can ensure the provision of threat and data protection for users accessing the public web, cloud services (SaaS, Email) and private applications (on-premises, IaaS) — regardless of location and device.

SASE offers network security that is people-centric, not site-specific, allowing users to connect only once for access to all IT-approved resources, regardless of location. SASE platforms rely on a dense worldwide network of points of presence (PoPs) in which users connect to the closest PoP via their browser or through a thin client. As a result, users enjoy an upgraded experience compared to using a corporate VPN.

Spectra Integrations: Proofpoint and CrowdStrike integration delivers best-of-breed threat intelligence sharing and analysis. Together, Proofpoint and Okta make security orchestration faster and easier by integrating best-of-breed solutions to provide accurate, timely response to credential phishing attacks.

Back to Contents

The Bigger Truth

As organizations embark on a journey to implement zero trust, they are faced with an architectural decision to stitch together existing security investments or rip and replace for more converged solutions from a single vendor. The security industry has long had a best-of-breed mindset, choosing the most effective, efficient solutions for individual security controls. IT complexity has been a key driver of this approach, with many organizations supporting hundreds of security controls across different operating units and geographies.

Although each organizations' security and operational needs are unique, a zero trust security model is achievable with careful planning, prioritization, prevention measures, and continuous monitoring. When considering a diversified, consolidated, strategic, or managed approach to zero trust, organizations with highly complex security infrastructure often choose a strategic approach that can provide zero trust advisory, technology, and support across the breadth of six elements, agnostic of deployment model and cloud providers. For these organizations, their existing investments with strategic platforms are being extended and expanded to achieve a zero trust security model.

The Spectra Alliance was created to support this strategic approach, offering users pre-build integrations that lead to zero trust. ESG recommends that organizations considering such an approach should explore the Spectra Alliance as a potential zero trust strategy.

CROWDSTRIKE | netskope | okta | proofpoint.

Back to Contents

> **Start as early as you can and make zero trust choices the first time rather than as a transition.** Our IT governance policies changed, we updated them and it is important to have those new processes in place to vet new security technology for zero trust. Where we are really doing zero trust is in our cloud and standing up least privilege requirements."
>
> *- Jonathan M, Cybersecurity Manager, US State and Local Government*