The Essential Guide to Zero Trust

splunk>
turn data into doing™

Table of Contents

What Is Zero Trust? 4

The Evolution of Zero Trust........ 5

The Zero Trust Model........ 6

The Splunk Data Analytics Journey for Zero Trust........ 9

Stage 1: Collect Relevant Data........ 12

Stage 2: Understand and Contextualize Your Data 13

Stage 3: Expand On Your Data........ 16

Stage 4: Enrich and Augment Your Data........ 18

Stage 5: Advanced Automation and Orchestration 19

Stage 6: Advanced Threat Detection........ 21

Zero Trust Requires an Ecosystem Approach........ 23

Your Zero Trust Ecosystem at Work: An Example........ 26

A Data-First Approach to Zero Trust........ 27

Now more than ever, organizations are turning to a zero trust strategy to secure their data and systems. Regardless of size or sector, zero trust is essential to any business in the wake of COVID-19. And high-profile breaches (see: SolarWinds), cloud migration and an ever-expanding attack surface mean that a shift in approach is all the more critical.

But this type of initiative can seem daunting. Especially when it involves rethinking how to tackle security across an entire organization — *as well as* every device, application and user that's connected to it. To further complicate matters, zero trust isn't limited to just traditional IT, and extends to operational technology/industrial control systems (OT/ICS) and the internet of things (IoT) — both popular points of compromise for hackers.

The good news? A zero trust model can radically improve your organization's security posture *and* minimize operational overhead by eliminating the sole reliance on perimeter-based protection. Instead of following traditional methods, zero trust establishes a certain level of trust at each access point — effectively securing users, assets and resources. This doesn't mean getting rid of perimeter security, however. Rather, it's an organizational shift in approach when it comes to protecting core assets.

Bottom line: Zero trust isn't *just* an architectural framework. It's a mindset that pushes organizations to rethink what's monitored, triaged and remediated. In this essential guide, we'll explore the driving forces that necessitate a zero trust strategy, as well as what that strategy entails, how it can be implemented, and — ultimately — how to reimagine what it truly means to be secure.

What Is Zero Trust?

The fundamental principle of zero trust is to secure an organization's data wherever it might live, while allowing only *legitimate* users and entities access to relevant resources and assets. With this mindset, every user, device and service that requires access to an organization's network is considered hostile until proven otherwise.

Simply put, the key here is to understand who wants access, what device the request is originating from, and then mapping that to access policies per application or asset. This amounts to a whitelist method for granting access, based on an employee's device, user credentials and behavior. Authentication needs to be continually applied at the device- and user-level for each session, ensuring continuous and adaptive authorization on a granular scale.

To break this down further, a successful zero trust security program must:

- Assume the network is always hostile.
- Accept that external and internal threats are always on the network.
- Know that the location of a network locality is not enough to decide to trust in a network.
- Authenticate and authorize every device, user and network flow.
- Implement policies that are dynamic and calculated from as many data sources as possible.

An example of what this looks like is an employee who's authorized to use an organization's case management system from a newly assigned device. The employee makes a request from that device and is granted access. Eventually, they download a driver from a website in an effort to be helpful. Since the device is continuously monitored in a zero trust strategy, the update is flagged.

This newly added component has altered the configuration — and therefore the trust score — of the device in question. Now when the employee attempts to connect to the system, their access could be denied, or downgraded, depending on their new trust score and associated policy. This shows how leveraging multiple factors (in this case, the combined scores of the user, device and resource) helps security teams reduce risk to enterprise resources dynamically. A zero trust system has the ability to factor in changing conditions for continuous evaluation, and continuous protection.

The Evolution of Zero Trust

Before zero trust was first defined by Forrester in 2010, security practitioners followed a network-based segmentation model, built on traditional network security solutions. This looks like a hardened perimeter, or a proverbial castle wall around an organization's network, housing all of its precious resources and data. But if a threat were to penetrate the network and breach the perimeter, a hacker could then have free reign, moving laterally across the network as well as any connected systems, compromising assets and causing irrevocable damage.

Enter de-perimeterization

Eventually, security teams started to move away from a network-centric approach, to an approach centered on the idea that any device, user or system — whether internal or external to the organization — should never be implicitly trusted, and access to all resources should be explicitly authenticated and authorized. However, up until recently, this was much easier said than done. Certain technologies simply lacked the necessary integration capabilities, limiting an organization's ability to centrally and holistically monitor the overall security of their organization's resources, creating further fragmentation and requiring a detailed implementation by security engineers.

Now, there are countless technologies available that revolve around access control — that is, a set of rules to determine who should be granted access to a restricted location and/or critical information. A zero trust architecture can stitch these systems together, reducing the complexity of managing multiple controls independently.

These technologies include (but are certainly not limited to):

- Identity and access management (IAM)
- Multi-factor authentication (MFA)
- Data loss prevention (DLP)
- Cloud access security brokers (CASB)
- Cloud infrastructure entitlement management (CIEM)

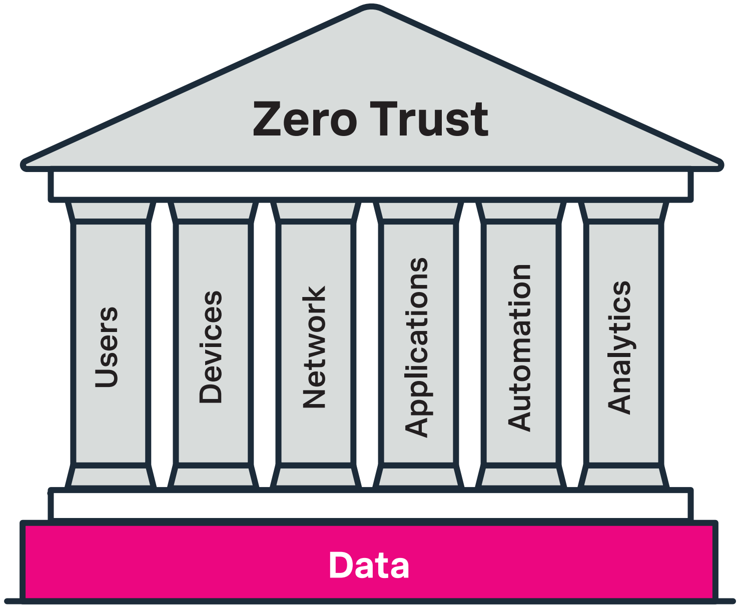
Thanks to these advances, zero trust has become easier to implement. COVID-19 also pushed organizations and companies around the world to accelerate their digital transformation. Overnight, employees were forced to work remotely, putting a significant strain on IT and security infrastructure. Compounded by the challenge of a dissolving perimeter and a growing attack surface, zero trust became an absolute global imperative.

The Zero Trust Model

The American Council for Technology and Industry Advisory Council (ACT-IAC) — a nonprofit, public-private partnership dedicated to improving government through information technology — lays out the six pillars of a zero trust security model, each of which are built upon a foundation of data.

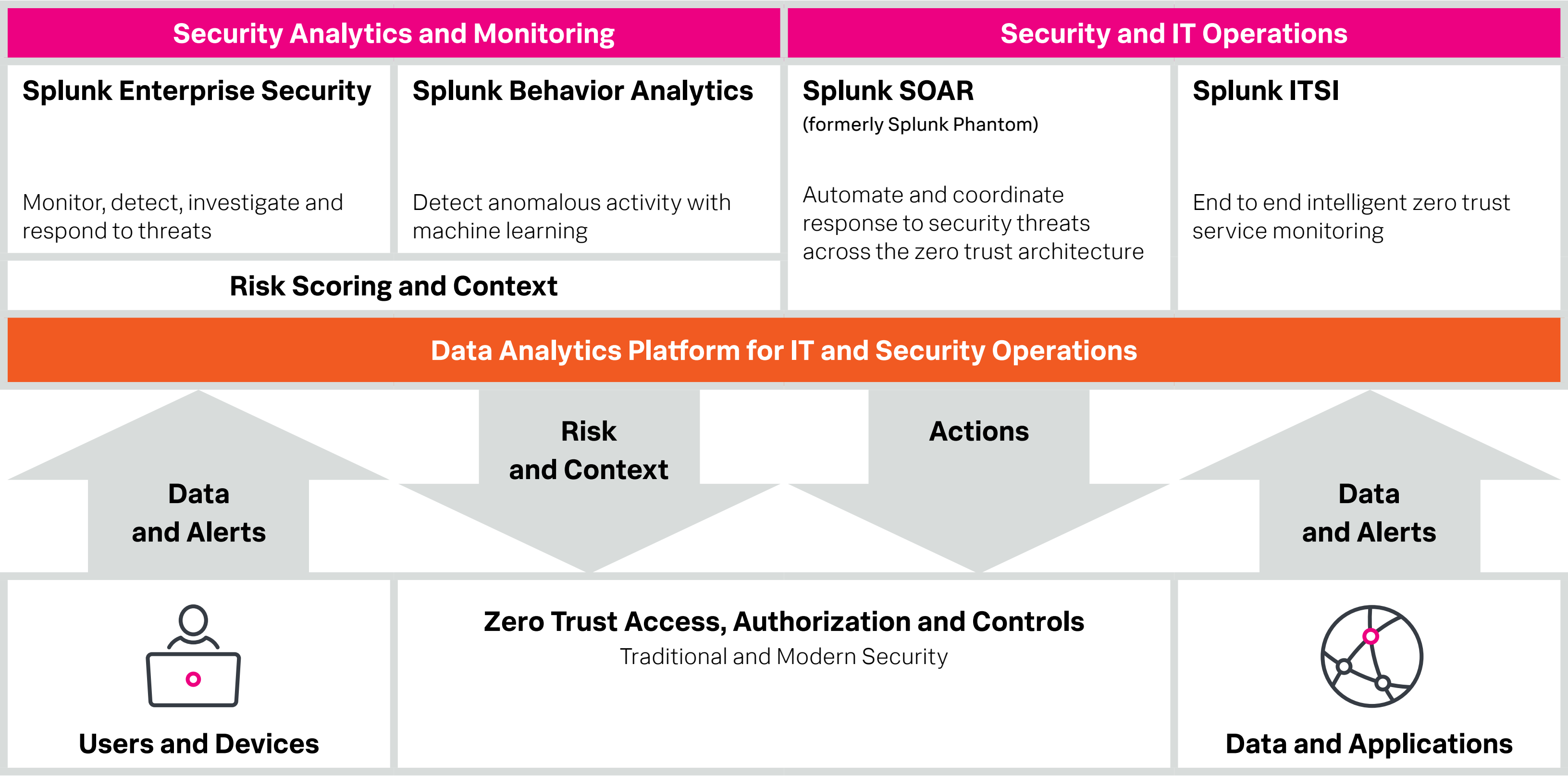
These are summarized as:

- **Users:** The ongoing authentication of trusted users, the continuous monitoring and validating of user trustworthiness to govern their access and privileges.
- **Devices:** Measuring the real-time cybersecurity posture and trustworthiness of devices.
- **Network:** The ability to segment, isolate and control the network, including software-defined networks, software-defined wide area networks and internet-based technologies.
- **Applications:** Securing and properly managing the application layer as well as containers and virtual machines.
- **Automation:** Security automation, orchestration and response (SOAR) allows organizations to automate tasks across products through workflows and for interactive end-user oversight.
- **Analytics:** Visibility and analytics tools like security information and event management (SIEM), advanced security analytics, and user and entity behavior analytics (UEBA) allow security experts to observe what's happening and orient their defenses accordingly.



Your friendly zero trust cheat sheet

- □ A zero trust model should authorize and authenticate user access to all assets and resources, and access should be given based on the company's corresponding policy and on a per-session basis.
- □ Zero trust controls need to be identified and aligned to your systems, users and data. These should be considered from two perspectives:
  - □ Security controls for securing internal/cloud infrastructure, networks, systems, applications and data — sometimes classified as the "object."
  - □ Security controls for the protection and authorization of users and endpoints when accessing resources. This should also include administrative access and is classified as the "subject."
- □ There should be a common set of policies, practices and protocols in place to manage the identity and trust score of users and devices across all systems, including external resources (e.g., software as a service).
- □ The management of zero trust controls need to be unified, and dynamic end-to-end access provisioned based on business-level logic, and not traditional security rules (e.g., IP-based controls).
- □ End-to-end data analytics should be established, providing monitoring and threat detection across the entire architecture, supporting both IT and security operations requirements.
- □ A centralized security posture is adopted, with contextualized risk profiling and advanced policy logic for access authorization.
- □ Existing security controls and processes need to be accounted for, in addition to their suitability and compatibility within the broader zero trust architecture.



Security Analytics and Monitoring

Security and IT Operations

Splunk Enterprise Security

Monitor, detect, investigate and respond to threats

Splunk Behavior Analytics

Detect anomalous activity with machine learning

Splunk SOAR

(formerly Splunk Phantom)

Automate and coordinate response to security threats across the zero trust architecture

Splunk ITSI

End to end intelligent zero trust service monitoring

Risk Scoring and Context

Data Analytics Platform for IT and Security Operations

Data and Alerts

Risk and Context

Actions

Data and Alerts

Users and Devices

Zero Trust Access, Authorization and Controls

Traditional and Modern Security

Data and Applications

Now that you're fully equipped with the history and basic tenets of zero trust, we're ready to move on. In the following sections, we'll focus on how building a modern security operations center (SOC) can support security monitoring for zero trust — and how Splunk can help organizations achieve their zero trust objectives in no time flat.

The Splunk Data Analytics Journey for Zero Trust

As organizations look to adopt a zero trust strategy, it's essential to monitor, detect and investigate security incidents relating to zero trust controls and policies — specifically the protections in place for users, systems, applications and data.

After many years of helping customers implement data analytics solutions — in addition to looking at industry best practices and the collective Splunk experience — Splunk has developed what we like to call the security data analytics journey.

This maturity model breaks down an organization's security journey into distinct stages. The goal is for each stage to cover specific objectives, while allowing for incremental, iterative improvements before moving on to the next phase of growth. Although this journey is focused on security outcomes, it also aligns with the development of IT monitoring capabilities through the reuse and rehashing of data.

This approach is perfectly suited to: **1.** Help your IT and security operations better align to a zero trust strategy, and **2.** Build a modern SOC that supports a zero trust architecture and bridges any existing gaps. The following sections will go through each stage of the data analytics journey as it aligns to the necessary steps, so you can address zero trust requirements in tandem with your IT and security operations.

The Splunk Security Data Analytics Journey

STAGE 6

Advanced Detection
Apply sophisticated detection mechanisms including machine learning

STAGE 5

Automation and Orchestration
Establish a consistent and repeatable security operation capability

STAGE 4

Enrichment
Augment security data with intelligence sources to better understand the context and impact of an event

STAGE 3

Expansion
Collect additional data sources like endpoint activity and network metadata to drive advanced attack detection

STAGE 2

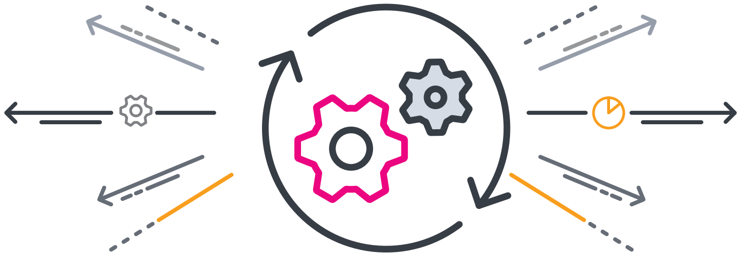
Normalization
Apply a standard security taxonomy and add asset and identity data

STAGE 1

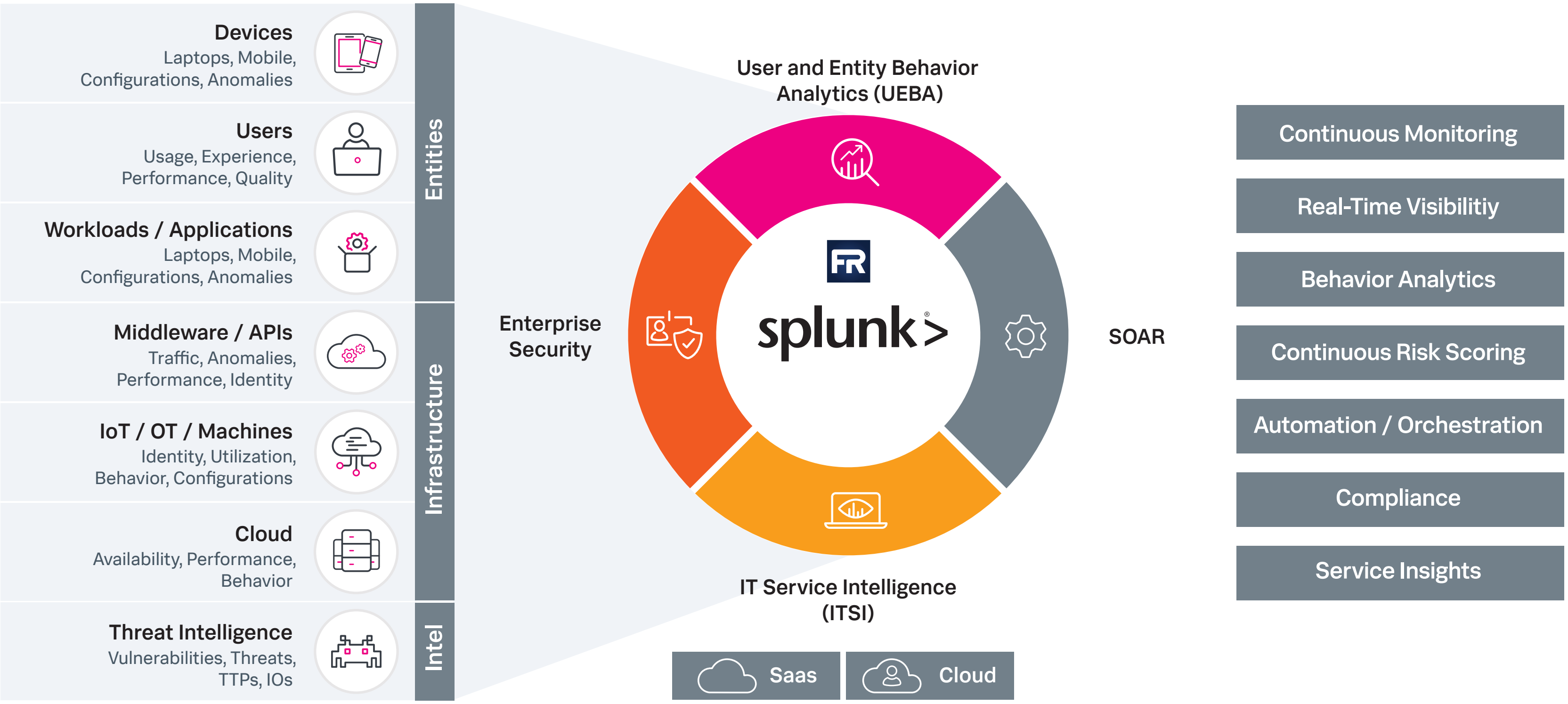
Collection
Collect basic security logs and other machine data from your environment

Throughout each stage of your zero trust journey, we'll cover how our suite of products aligns to the various requirements for security and IT monitoring for zero trust. These products include:

- Splunk Enterprise: Data Analytics and Investigations Platform
  - Scalable data analytics platform; supports IT, security and fraud use cases for zero trust architectures.
  - Ability to ingest a broad range of structured and unstructured data.
  - Comprehensive partner ecosystem; includes zero trust solutions to support integration, as well as rapid data source onboarding and normalization.
- Splunk Enterprise Security: Security Information and Event Management (SIEM)
  - Extensive security monitoring and detection use case library, supported by Splunk Security Essentials (SSE) and Enterprise Security Content Update (ESCU).
  - Key frameworks to support the enrichment and contextualization of asset and identity data, risk scoring and security posture in support of zero trust objectives.
  - Risk based alerting (RBA) helps with advanced risk scoring and multi-indicator detections aligned with the MITRE ATT&CK framework. Looks across zero trust controls for a sequence of activity that could indicate malicious behavior.
- Splunk User and Entity Behavior Analytics (UEBA)
  - Out-of-the-box, unsupervised machine learning for advanced behavioral detection and automatic identity resolution.
- Splunk SOAR for Security Orchestration, Automation and Response (formerly Splunk Phantom)
  - Comprehensive case management, incident investigation, orchestration and automation to respond to security and service incidents across a zero trust architecture.
- Splunk IT Service Intelligence (ITSI)
  - End-to-end service monitoring of zero trust controls and the underlying infrastructure of the related applications and services.



Splunk Solution Overview for Zero Trust IT and Security Operations



Devices
Laptops, Mobile, Configurations, Anomalies

Users
Usage, Experience, Performance, Quality

Workloads / Applications
Laptops, Mobile, Configurations, Anomalies

Middleware / APIs
Traffic, Anomalies, Performance, Identity

IoT / OT / Machines
Identity, Utilization, Behavior, Configurations

Cloud
Availability, Performance, Behavior

Threat Intelligence
Vulnerabilities, Threats, TTPs, IOs

Entities

Infrastructure

Intel

User and Entity Behavior Analytics (UEBA)

Enterprise Security

splunk>

SOAR

IT Service Intelligence (ITSI)

Saas

Cloud

Continuous Monitoring

Real-Time Visibilitiy

Behavior Analytics

Continuous Risk Scoring

Automation / Orchestration

Compliance

Service Insights

Stage 1: Collect Relevant Data

First, identify your organization's most critical assets — specifically what you need to protect and monitor in order of priority. Once you've triaged your assets, you'll have a much better idea of where to allocate resources, and where to start ingesting data from.

Because zero trust consists of many different types of technologies, there's a good chance your organization already relies on some of these systems. This will be an important source of data for IT and security monitoring, and the very foundation of a comprehensive end-to-end zero trust program.

Examples of these technologies include:

- Next generation firewalls (NGFW)
- Software defined networking (SDN) and micro segmentation solutions
- Cloud access security brokers (CASB)
- Remote access
  - Virtual private network (VPN)
  - Virtual desktop infrastructure (VDI)
  - ZT access (ZTA)
- Identity access management (IAM) and directory services
- Multi-factor authentication (MFA)
- Privileged authentication management (PAM)
- Endpoint detection and response (EDR)
- Security posture solutions (e.g., patch and vulnerability management)
- Web proxy, web filtering and secure web access services
- Data loss prevention (DLP)
- Secure access service edge (SASE)
- Unified endpoint management (UEM) and mobile device management solutions

Elements that make up the underlying infrastructure for systems and services — like storage and networks, as well as the components that support IT administrative functions — are also important data sources, and should be considered during this phase.

Examples include:

- **Network:** The data center and cloud networking infrastructure, like switches, routers, load balancers, as well as any virtualized networking services.
- **Storage:** The data center and cloud storage systems and services, like storage arrays, system disks, network-attached storage (NAS/SAN) and cloud storage services.
- **Compute:** Data center and cloud computing resources, including the monitoring of physical and virtualized compute and associated operating systems.
- **Administrative:** Systems and applications supporting administrative functions such as monitoring systems, jump hosts, administrative authentication and privileged access control.

This may seem like a lot of work, but a key part of the Splunk data analytics journey is to take incremental steps based on each individual system or service, as well as the specific use case you need to implement at the time. By identifying and defining your most critical assets and entities, you form the very basis for contextualization and prioritization of IT and security incident alerting. And as you build out your data sources, you'll have the ability to reuse this data as you progress along the maturity curve.

Stage 2: Understand and Contextualize Your Data

Contextualizing your data is key to any zero trust strategy. To understand your data, you have to implement a standard taxonomy across all data sources — otherwise you're left with a whole lot of noise. Creating a taxonomy for your data will eliminate a lot of confusion, especially as you continue to level up on your security journey.

One example is how firewall vendors use different log formats and data structures across systems. In order to support centralized monitoring, firewall log data needs to be structured in a way that normalizes field names and values, putting them into a consistent format.

To structure or not to structure? *That* is the question

Splunk has developed a common information model (CIM), an open and extensible approach to creating a common taxonomy. Splunk CIM is a way to structure and standardize field names and values, which are pulled from raw data, and subsequently turned into data models that cover a broad range of categories. With Splunk, this is done post-ingestion, and without modification to the raw data itself.

This means you can continue to update data structures as your requirements change, *without* modifying your raw data or having to go through the hassle of re-ingesting everything. There's also the added benefit of data model acceleration — where you can accelerate datasets with the help of a pivot search — which increases search performance of structured data. Ultimately, results that are integral to the overall health of your zero trust model are returned quickly and predictably.

Splunk CIM supports these native monitoring and detection capabilities within Splunk Enterprise Security (ES), and can be applied to all of your dedicated zero trust data sources. Data onboarding and normalization is also supported by our Splunk partner and user ecosystem, featuring an extensive range of Splunk add-ons that customers can install.

Bottom line? Splunk add-ons support countless zero trust data sources, and are continually updated to support new and changing capabilities.

The new normal(ization)

Now, we can start to implement use cases that are designed for normalized data. An excellent starting point for security detections is the use case library provided by Splunk Security Essentials (SSE). SSE has a comprehensive range of use cases that map to each phase of the security analytics journey.

Better yet, there's now a new category in SSE which identifies and maps zero trust use cases to each stage of your journey by aligning to the MITRE ATT&CK framework. The MITRE ATT&CK framework provides an extensive knowledge base for real-world threat tactics and techniques, and is widely used by security teams.

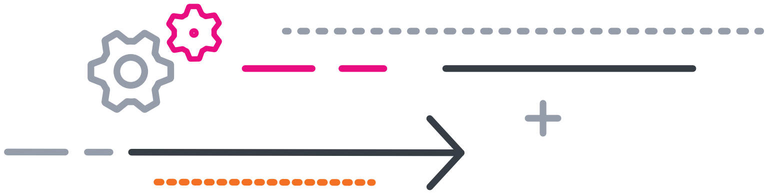
We put the MIGHT in MITRE ATT&CK

By evaluating the threats that a zero trust strategy aims to prevent, we've identified a comprehensive list of security use cases based on related MITRE ATT&CK tactics. Given the complexity and scope of a complete zero trust implementation, this can help organizations augment a controls-based approach with suitable security detection and monitoring use cases for zero trust.

Just remember: This guidance should be considered in the context of a broader security monitoring strategy, as plenty of other threat types *can* and *will* apply in specific situations.

The following MITRE ATT&CK tactics have been used to categorize some of the primary security detection use case in SSE for zero trust:

- **Initial access:** The adversary is trying to get into your network.
- **Persistence:** The adversary is trying to maintain their foothold.
- **Privilege escalation:** The adversary is trying to gain higher-level permissions.
- **Credential access:** The adversary is trying to steal account names and passwords.
- **Lateral movement:** The adversary is trying to move through your environment.
- **Exfiltration:** The adversary is trying to steal data.



And the following use cases can apply to stage two of your security journey (the normalization of data), and are based on foundational data sources like authentication, network and endpoint data (onboarded during stage one):

- Account management changes
- New account creation
- Changes to security policies or controls
- Brute force authentication activity
- Clearing of administrative or security logs
- Unauthorized system configuration changes

Since data normalization is part of this stage, we can look to Splunk Enterprise Security to monitor and report on zero trust-related activities. These include:

- Endpoint and server malware, and system configuration change monitoring
- Endpoint and server vulnerability, and patch management
- User access and account management
- User web activity monitoring
- Network traffic monitoring

Now, we can begin to incorporate information like the risk profile of systems we're protecting, as well as relevant context around user identity. This is a key part of security analytics, as it forms the basis of risk scoring and the prioritization of security alerts. And since you've already identified what assets and entities you need to protect (as discussed in stage one) you can use this information for additional color.

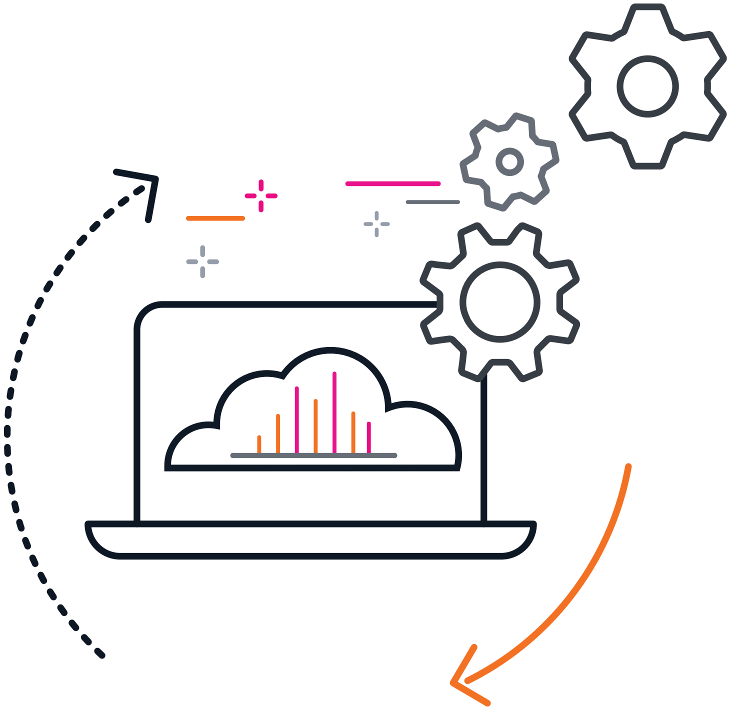
Examples of important contextual information include:

- **Asset risk profile:** What is the business impact of an incident affecting this asset? What is the likelihood of an incident affecting this asset? What is the security posture of this asset? What is the sensitivity or importance of the data processed or contained within this system? What types of users typically access or rely on this system?
- **Identity risk profile:** How important is this identity? Is it a service account, administrative account, executive level user account or contractor account? Is it an account that is more likely to be targeted or is it inherently untrustworthy? What will the impact be if this identity is compromised? Is the user a flight risk?

The asset and identity framework built into Splunk ES is integral to this stage of exploration, and forms the very basis of risk scoring. Every asset or identity logged in ES maintains a record over time, based on security events, their severity and the importance of the asset or identity in question. In the final stage of your security journey (advanced detection) we'll continue to build on these principles with the introduction of risk based alerting.

Data sources which are ingested, aggregated and structured into the asset and identity framework include:

- Configuration management databases (CMDB)
- Network asset discovery tools
- Directory and authentication services
- Human resource systems
- Cloud environments



Stage 3: Expand On Your Data

More often than not, the continuous monitoring of security controls will fail to detect advanced security threats. This is why security monitoring should look at how target systems function, as well as what authorized use looks like. A holistic view of systems, data and users also needs to be established — and that includes behavioral and infrastructure monitoring.

Why? Because zero trust can't always stop fraud, insider threats or advanced attacks that occur via authorized means (e.g., a compromised user account). But a zero trust strategy *can* contain an incident, and restrict the scope of any potential damage. If we're looking in the wrong place, however, there's a good chance this type of threat won't be detected in time. By considering zero trust policies and how an authorized user should behave, we can gain insight into anomalies we *should* be monitoring, so we can better detect malicious access.

More data = Less stress

This means that additional data sources — outside of just security controls — should be ingested to provide further visibility into user behavior. One example is to pull network flow data, and to correlate network activity with application and process activity. This would help with the detection of unauthorized applications using authorized network communications, and could even help identify lateral movement across multiple applications and user accounts.

Even if we have good monitoring coverage thanks to the controls and policies governing zero trust, we still need to pay close attention to what authorized users and systems do once they're granted access. Looking beyond what our security controls tell us can help with situations where credentials may have been compromised or devices hijacked.

The following types of data sources can help detect these deviations across user and device behavior:

- **Endpoint:** Understand application and process execution, file integrity monitoring, network connections using extended endpoint detection and response (EDR) capabilities or tools like Sysmon and osquery.
- **Application:** Start with business-critical applications like financial systems, systems processing sensitive data, customer data, and logs that record user activities.
- **Database:** Understand audit and transaction logs to identify unusual patterns of behavior, modification or deletion of records, and potential unauthorized access to sensitive or restricted records.
- **Cloud:** This mainly focuses on software as a service (SaaS) business applications for user monitoring, but also looks at infrastructure as a service (IaaS) and platform as a service (PaaS) environments in order to detect suspicious administrative activities that could compromise zero trust policies.
- **Cloud file storage services:** Looks at the movement of sensitive data and unusual patterns of data movement.

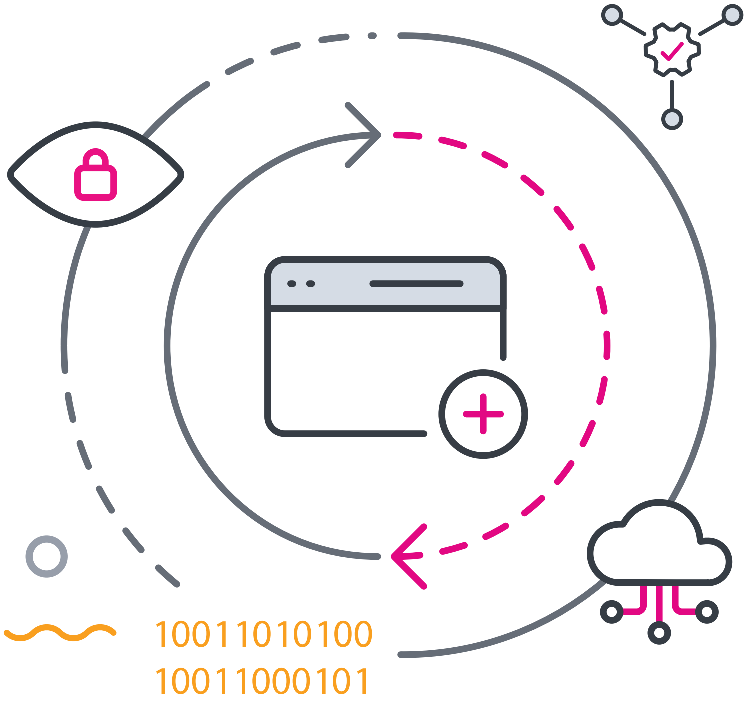
Expanding on the initial detection and monitoring initiated in stage two, we can continue to add to these use cases with more advanced detections provided by data sources onboarded in stage three. This involves the use cases offered by SSE, along with use cases from Splunk Enterprise Security and the Enterprise Security Content Updates.

Analytic stories

ESCU use cases are defined as “analytic stories,” which support the full incident and detection lifecycle, and include a narrative around the use case, details specifying the data sources, as well as searches designed to support the detection and investigation of the incident.

Examples of use cases for stage three include:

- Lateral movement
- Anomalous time of day or location for user authentication or access
- New user access to system(s) or application(s)
- New removable media device
- New local account creation
- Interactive use of default, system and services accounts
- Unusual, rare or never before seen processes/applications
- Unusual command line activity (obfuscated powershell)
- Unusual or rare cloud application usage (file sharing)
- Endpoint changes and posture (installation of software, modification of system files)



Stage 4: Enrich and Augment Your Data

During this stage, we'll look at data sources that provide even more context, like threat intelligence, information from vulnerability and patch management tools, and attack surface management solutions.

The lay of the (threat) land(scape)

Threat intelligence (TI) helps us identify indicators of compromise (IoCs) across zero trust controls and protected systems. Users can access these systems in real time via the Splunk ES threat intelligence framework, or as part of an enrichment playbook using Splunk SOAR's automation capabilities.

This helps us understand the threat landscape as it relates to the systems and users we're protecting, and to also identify known IoCs that would otherwise go undetected by zero trust security controls. Examples of this include IP addresses, URLs or file hashes associated with phishing activity, or identifying information relating to an SSL certificate known to be used for malicious purposes.

Secondly, understanding the posture of protected assets — as well as the systems used to access these resources — helps with risk scoring and security incident prioritization, as well as access authorization. For example, user systems with missing or insufficient system patches can have their access to critical systems limited, and security incidents connected to known vulnerabilities can be prioritized.

On top of all this, attack surface management solutions can help with overall security posture — specifically focusing efforts on optimizing security controls and ensuring end-to-end visibility. If we know we have gaps in our controls, we can look to mitigate or implement enhanced monitoring.

In summary, the enrichment stage helps with:

- **Real-time threat intelligence:** The Splunk Enterprise Security TI framework ingests and curates multiple TI feeds, including commercial and open source, and relies on transport protocols like STIX and TAXII. This is subsequently used to match IoCs across various zero trust data sources, proactively identifying known threats.

  Examples of typical TI IoCs include:

  - IP addresses
  - FQDN/URLs
  - File names and file hashes
  - SSL certificate information

- **Monitoring of the threat landscape:** The Splunk Enterprise Security TI framework also provides monitoring capabilities to better understand the threat landscape and trends specific to your environment. TI monitoring looks at the rate of occurrence across different types of threats, as well as IoCs within your environment and different feeds.
- **Real-time security posture:** Splunk Enterprise Security and Splunk CIM provide a range of capabilities to ingest and utilize data from vulnerability and patch management solutions. This data can be used to create an enterprise-wide view of aggregate data around security posture, while also providing context for prioritization of security incidents.

Stage 5: Advanced Automation and Orchestration

Now that we've established a strong foundation for monitoring and security detections with a veritable triple threat — that is, centralized, normalized and enriched data — we can move onto investigation and response.

Splunk SOAR relies on orchestration and automation to streamline and accelerate incident investigation and remediation. Using automation to rapidly contain and resolve security incidents across zero trust controls, Splunk SOAR can be executed via advanced playbooks or unique requests.

Put the PEP back in your step

These playbooks rely on "decision logic" to perform different actions based on the context of the response required. This capability allows for advanced policy logic to extend to zero trust policy enforcement point (PEP) and network access control (NAC) capabilities, incorporating real-time risk scoring to further improve zero trust authorization.

Splunk SOAR can also define standard operating procedures in alignment with industry frameworks like NIST 800-61, so analysts can follow the type of incident they're managing through the corresponding workbook or case template. This allows the analyst to focus on what they do best — interpret data.

Let your data SOAR

Just as we took a phased approach to data analytics, SOAR requires a similar treatment:

1. First, identify manual, repetitive tasks that analysts usually perform. This is where the most value will be gained from automation.
2. Understand and document the entire process, including various technology touchpoints, as well as the time it takes for each step. This process can be documented using Splunk SOAR workbooks.
3. Develop a process flow diagram, including any steps involving decisions or approvals. This will form the basis of the playbook, automating the process. Identify any sections of the process that may be suited to modularization for reuse as sub-playbooks.
4. Identify, install and configure Splunk SOAR applications to support integration with certain components.
5. Start out using the process defined in workbooks. Investigate and respond to incidents, and leverage capabilities through the use of ad-hoc actions.
6. Build and refine a playbook to gradually automate as much of the process as possible, creating modular playbooks where there's potential for reuse.
7. Review playbooks and monitor analyst performance over time to understand what's been successful. Look for other opportunities for improvement.

Some high-level examples of zero trust use cases for Splunk SOAR include:

- Workbooks/case templates defining zero trust-related incident response and investigation. Examples include:
  - Account compromise
  - Data breach
- Playbooks providing automation of zero trust-related incident response. Examples include:
  - Active directory reset password/lock account
  - Compromised email containment and response
  - Phishing email investigation and response
  - Lost/stolen device containment
  - Malicious insider containment
  - Malware containment and response
  - Malicious web resource containment and response

And it gets better. Analysts no longer need to log on to zero trust controls directly. Splunk SOAR integrates with privileged access management (PAM) solutions, allowing the user to perform actions from within.

It's also possible to implement a level of advanced authorization beyond zero trust PEP/NAC solutions. Now, by looking at risk posture and scoring in real time, we can draw on even more information before authorizing user access — thereby expanding on traditional zero trust access and authorization policies. This gives us the ability to combine and assess the risk scores of both the user *and* the system they're trying to access, providing a greater understanding of that endpoint's risk profile.

Automate manual SOC tasks

During (and even after) the authorization phase, Splunk SOAR can be used to evaluate the risk profile of assets and identities in Splunk ES, and can determine if access should be granted or revoked, in addition to any other actions that should be taken. This can then be shared with the zero trust NAC or policy engine, and used to ultimately authorize, deny or revoke access. In the event that access is denied, Splunk SOAR can take further action, depending on the reasons for denying access in the first place.

Examples include:

- User access is denied and a notification issued based on an elevated risk score.
- User access is restricted if unusual or risky behavior is exhibited after initial authorization.
- Initiate system vulnerability or inventory scans for assets that show evidence of unusual behavior after authorization.
- Create IT support tickets automatically for systems out of compliance where access has been denied.
- Automatically remediate activities such as patching, disabling unauthorized software/services or (re)applying security controls.

Stage 6: Advanced Threat Detection

We're finally at the last stage of establishing a zero trust architecture. Now, we're going to define advanced security detections with risk based alerting (RBA). This will help guarantee the fidelity of the threats in your queue as well as minimize the overall volume of alerts. We can also begin to augment the capabilities of Splunk Enterprise Security with Splunk UEBA.

The goal here is to think about: **1.** The policies surrounding zero trust, **2.** What users typically do with the systems they have access to, and **3.** How to identify patterns of behavior that could be indicative of unusual or malicious activity.

First, you'll need to build on the detection use cases from earlier, so you can look across the different phases of a security incident (i.e., the kill chain), and start to use multiple indications of suspicious activity to generate an alert.

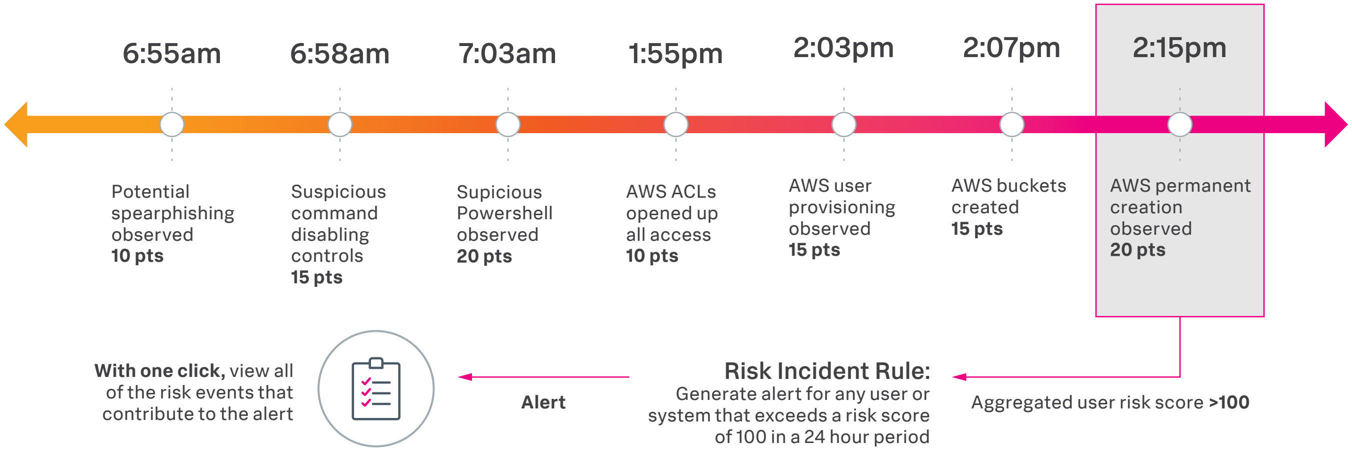
Save the day with RBA

With risk based alerting, instead of generating an alert at the first sign of a potential threat, a record of the event will simply be created. Once this event is logged, any further indication of malicious activity will be flagged. This means we can now see the sequence or pattern of events in relation to the asset or identity in question, neatly wrapped up into a single alert.

In the following example, we can see how data exfiltration was preceded by a number of unusual events. Before RBA, each event would generate a unique alert, which would (most likely) end up lost in the ether. However, by looking across the kill chain and using multiple indications, we're able to generate a single alert with a higher level of confidence.

Risk Based Alerting for Zero Trust

Multiple zero trust related events become context that informs high-fidelity alerts


6:55am
Potential spearphishing observed
10 pts
6:58am
Suspicious command disabling controls
15 pts
7:03am
Supicious Powershell observed
20 pts
1:55pm
AWS ACLs opened up all access
10 pts
2:03pm
AWS user provisioning observed
15 pts
2:07pm
AWS buckets created
15 pts
2:15pm
AWS permanent creation observed
20 pts
Aggregated user risk score **>100**
Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period
Alert
With one click, view all of the risk events that contribute to the alert

We can also introduce more advanced risk scoring capabilities that dig deeper into how alerts are prioritized. For example, the standard risk scoring framework for Splunk ES looks at the importance of the asset or identity, and also factors in the severity of the alert to determine the rolling risk score.

With RBA, we can include additional layers of dimension to help with zero trust. Examples of relevant use cases include:

- Techniques across multiple zero trust MITRE tactics in a 24-hour period.
- Multiple zero trust MITRE techniques from a single tactic in a 24-hour period.

Even though RBA and UEBA operate differently, they're both similar in that they use multiple indications to home in on suspicious or malicious activity. Thanks to the many points of reference these tools draw on, they're better able to generate higher fidelity alerts while reducing the number of false positives.

User and Entity Behavior Analytics

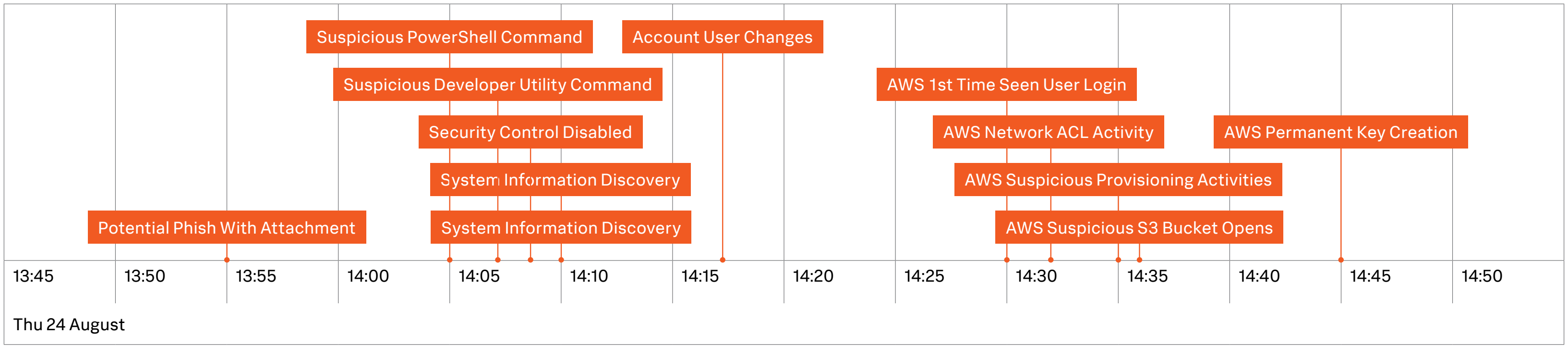
Unsupervised machine learning with Splunk UEBA helps us look for deviations across user activity, devices and applications. In many cases, these events are harmless occurrences (if unusual). But by using a similar approach to RBA, UEBA looks for patterns and sequences that relate to the different stages of a security incident, and automatically groups these anomalous events into a single alert or threat.

As with RBA, this serves to increase the fidelity of the alert, while simplifying analysts' efforts around the manual identification of associated events. Beyond behavioral analytics, the capabilities provided by Splunk UEBA also help with contextual enrichment and the mapping of user activity to the systems and data they're accessing.

Examples of a behavior-based approach to zero trust (which applies to insider and advanced threats) include:

- Data exfiltration by a compromised user account
- Data exfiltration by internal actor or flight risk user
- Advanced lateral movement detection
- Advanced privilege escalation

Zero Trust Threat Timeline View With RBA



Zero Trust Requires an Ecosystem Approach

Achieving a comprehensive zero trust policy involves a range of integrated components. Together, these controls provide the necessary data and insights for centralized monitoring.

By aligning zero trust methodologies to Splunk's ecosystem of partners, we can dramatically improve organizations' security posture and their overall security operations.

Read on to discover the capabilities of our zero trust partners, and how they can help you realize your zero trust goals.

Zscaler

Zscaler — one of our key strategic partners — is a leading security provider and innovator that securely connects users to the internet, as well as a host of private applications. Zscaler's Zero Trust Exchange is a cloud-native proxy architecture that directly connects users and applications to company resources, without creating any additional, undue exposure. Zscaler augments this architecture with Security Sockets Layer (SSL) inspection, strong authentication and rich policy-based controls.

Two of their main zero trust solutions are:

Zscaler Internet Access (ZIA) provides comprehensive security for users connecting to the internet, regardless of where they are. Zscaler's service is delivered from 150 data centers globally, giving users a fast, secure and hassle-free experience.

Zscaler Private Access (ZPA) promotes seamless, least-privilege access to both traditional and cloud-based applications for local and remote users — all without the complexity of traditional network segmentation and remote access solutions. The attack surface of applications is significantly reduced as they're hidden from public channels.

Splunk ingests Zscaler's high-fidelity telemetry with an out-of-the-box, cloud-to-cloud integration, giving security teams visibility into their cloud and network traffic, and helping them detect and eliminate emerging threats across the enterprise. The Zscaler API also allows security analysts to take coordinated action across the Zscaler platform and other security tools using Splunk SOAR, orchestrating user access and policy management via an application and technology add-on available via Splunkbase.

DTEX Systems

DTEX — the world's first and only Workforce Cyber Intelligence Platform — captures behavioral telemetry from across endpoints, producing dynamic "indicators of intent" and delivering holistic, real-time awareness regarding organizations' activities — all without invading personal privacy.

Thanks to complex scoring frameworks, DTEX can help you see, understand and act on contextual intelligence, and betters positions your organization to stop insider threats, prevent data loss, maximize software investments and protect your workforce. This level of visibility is critical when it comes to advanced insider and external threat detection, and provides an extensive source of data for behavioral anomaly detections.

For better implementation of advanced zero trust-related security detections and monitoring use cases, check out the DTEX-Splunk integration on Splunkbase, available as an application add-on.

CloudKnox

Due to the many new identities and policies across cloud-native services, it's become increasingly difficult to manage and secure different types of users and their level of access. Now, there's a huge gap in permissions granted versus permissions used, with most identities using <5% of high-risk permissions. This means it has become that much harder to enforce least privilege policies, exposing organizations to high risk, as well as the inability to manage zero trust access appropriately.

Which brings us to the CloudKnox Permissions Management Platform — a multicloud/hybrid-cloud permissions management and monitoring platform that protects critical-cloud infrastructure resources and identities by providing comprehensive visibility, automated remediation and continuous monitoring of permissions. With the CloudKnox patented "Activity Based Authorization" technology, the CloudKnox platform enables organizations to implement zero trust policies across all clouds with a single operating model. CloudKnox supports VMware vSphere (both on-prem and in the cloud), AWS, Azure and GCP.

CloudKnox is a Splunk strategic security partner for zero trust, supported by the Splunkbase add-on. The CloudKnox Permissions Management Platform has been deployed and integrated with Splunk across many enterprise organizations globally, including countless Fortune 500 companies.

Okta

Okta is a cloud-native, trusted platform for securing every identity, from customers to employees. More than 10,000 organizations trust Okta's identity solutions to sign in, authorize, and manage user access to critical applications and data across hybrid architectures, supporting a key aspect of an overall zero trust approach. The authentication and authorization data along with the context of identities from Okta provides a rich source of information to support the security monitoring requirements for zero trust with the Splunk approach. Through the existing integration with Splunk — provided by the Okta add-on available via Splunkbase — customers are able to quickly onboard and utilize their data in support of zero trust objectives.

Illumio

With their market-leading approach, Illumio has transformed security by helping organizations build a map of their applications, connectivity, endpoints and workloads, implementing micro-segmentation for zero trust, so only trusted communications are happening across cloud, hybrid, multicloud and on-premises. Discover Illumio's extensive zero trust capabilities, including comprehensive network security telemetry, by downloading the llumio app available on Splunkbase. The application provides advanced monitoring and reporting capabilities to support IT, security and compliance teams, and includes enhanced visibility across application traffic in Splunk, so you can quickly quarantine suspicious workloads with a single click.

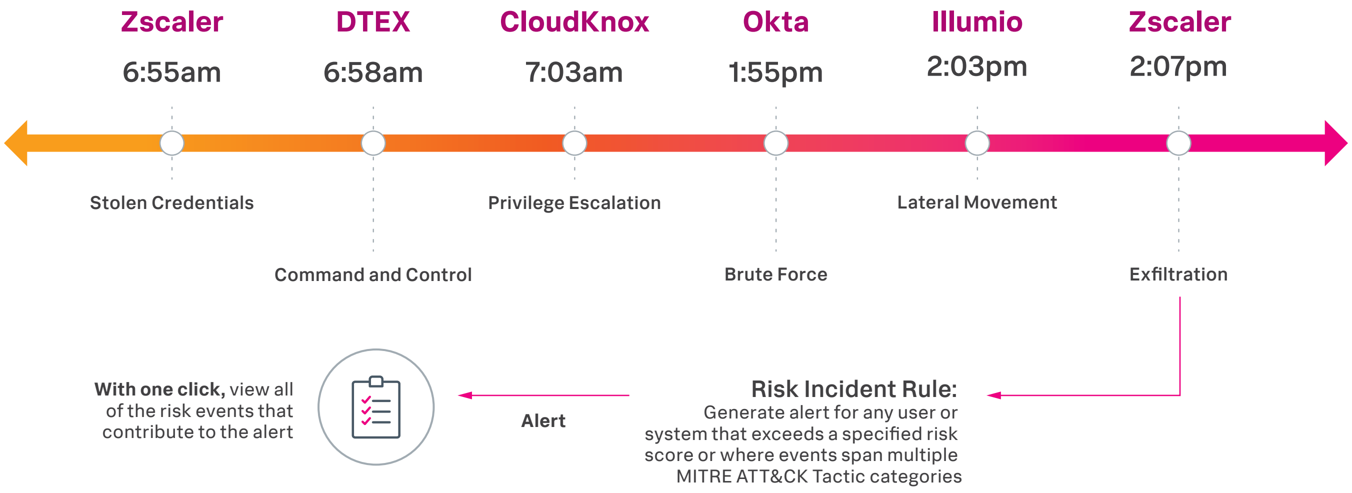
Your Zero Trust Ecosystem at Work: An Example

If we consider the MITRE ATT&CK categories we've mapped out — in addition to the many different stages that we've identified as part of your security journey — we can see how the zero trust technologies detailed previously support each use case. The following diagram provides a practical example of what's possible with this joint approach. Each of these partner solutions provide broad coverage to support the detection of these zero trust-related MITRE ATT&CK tactics, and can be combined with other sources of data for better visibility.

- **Initial Access:** Zscaler Private Access provides the telemetry required to detect suspicious or anomalous access to protected applications where valid credentials may have been stolen or hijacked.
- **Persistence:** The granular endpoint data from DTEX helps with the detection of unrelenting techniques used by attackers trying to establish a foothold with command and control.
- **Privilege Escalation:** Through the advanced monitoring capabilities provided by CloudKnox, we can detect changes to administrative or developer privileges across hybrid-cloud environments, such as anomalous use of valid cloud administrative credentials.
- **Credential Access:** Okta provides detailed authentication and authorization data which enables Splunk to detect anomalous activity, potentially indicative of suspicious credential access such as brute force attacks.
- **Lateral Movement:** With Illumio's approach to microsegmentation, providing granular visibility of network activity across a hybrid environment, we're able to detect attempted or successful lateral movement techniques.
- **Exfiltration:** Zscaler Internet Access supports monitoring of web activity which enables anomaly detection with Splunk for potential exfiltration of data over a broad range of web services.

Looking across the MITRE ATT&CK Tactic Spectrum

Multi-Source, Multi-Indicator, High Fidelity Alerts for Zero Trust using RBA

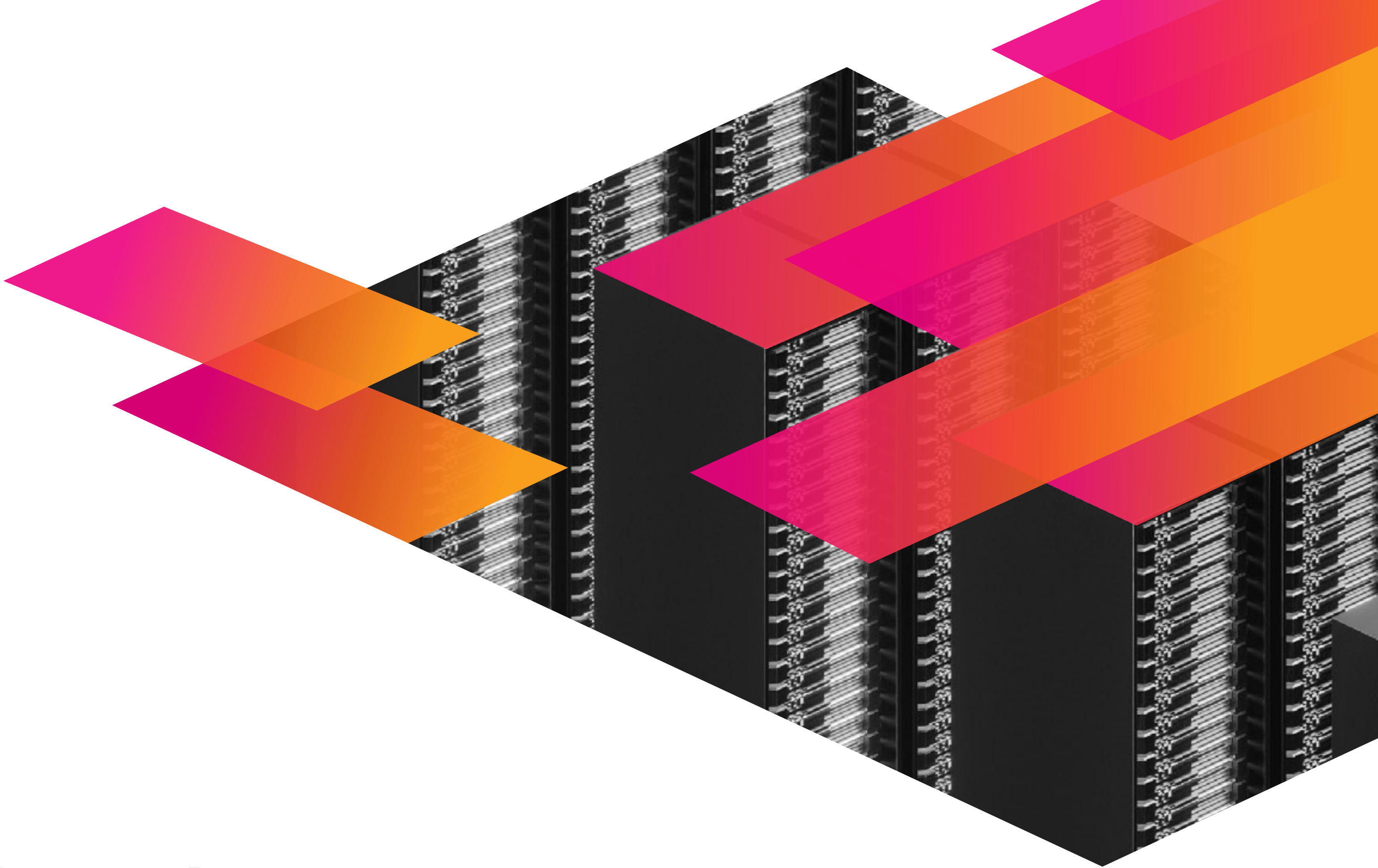

Zscaler
6:55am
Stolen Credentials
DTEX
6:58am
Command and Control
CloudKnox
7:03am
Privilege Escalation
Okta
1:55pm
Brute Force
Illumio
2:03pm
Lateral Movement
Zscaler
2:07pm
Exfiltration
Risk Incident Rule:
Generate alert for any user or system that exceeds a specified risk score or where events span multiple MITRE ATT&CK Tactic categories
Alert
With one click, view all of the risk events that contribute to the alert

A Data-First Approach to Zero Trust

This brings us to the end of your journey to zero trust. The key thing to remember is that there are countless benefits to a data-first approach to security, especially when it comes to building a zero trust architecture.

Data is at the center of any successful strategy, especially a successful *security* strategy. But all too often, the systems and structures we rely on end up trapping or segmenting our data — making it that much harder to extract its immense value.

The good news? You can remove these barriers and unleash a gold mine of insights and opportunity with the help of data analytics, in combination with a real understanding of your organization's zero trust policy, roles and resources. Thanks to the flexibility and openness of the Splunk portfolio, teams can now connect disparate technologies and take precise action — leading to better, faster and more effective decisions across the enterprise — and ultimately, a steadfast zero trust strategy.



From Zero to (Splunk) Hero

Regardless of where you're at on your zero trust journey, Splunk can help you stay one step ahead of new and existing threats. Discover how to modernize your security operations and improve your organization's security posture by downloading Splunk Security Essentials today.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2021 Splunk Inc. All rights reserved.

21-18251-Splunk-The Essential Guide to Zero Trust-EB-109

splunk>®
turn data into doing™