Monitoring Access Risk

Duo enables 800+ million secure authentications per month across more than 40,000 customers. By analyzing this data to create statistical and contextual baselines, Duo Trust Monitor highlights cases of anomalous or risky access.

THE CHALLENGE:

Detecting Malicious Access and Hardening Policy

In the past 10 years, the adoption of access management solutions like multi-factor authentication (MFA) and single sign-on (SSO) have helped limit the impact of weak or compromised credentials. Organizations leveraging these solutions are making important strides to harden their defenses against phishing and other credential-based attacks.

However, account takeover is still the most common vector to a breach. Security policies based on hard rules can potentially limit the scope of an attacker's presence, but policies are only as knowledgeable as the person invoking them.

Without proper analysis into the pattern of authentic and normal access in an organization, companies are missing important insight into more persistent or seemingly benign forms of compromise.

For example, without context around a salesperson's typical access patterns, it may be unclear when user credentials suddenly attempt access from a strange location or unexpected device.

Compromised credentials "sniffing around" the perimeter may go unnoticed if contextual data isn't ingested and analyzed.

What's more, organizations may not update and harden policy to reflect actual user behavior patterns. Companies often set and forget policy when initially deploying a security control. While certain policy is better than none, policy that doesn't evolve with the actual data of the business will always be less secure than it could be.

Duo Trust Monitor events can be easily exported via API to other security tools, including:

THE SOLUTION:

Duo Trust Monitor

Duo Trust Monitor creates a baseline of normal user and device access within a corporate environment. Deviations from this baseline can be used to highlight suspicious activity like account takeover. Visibility into normal and atypical access patterns also enables stronger, more granular access policy.

01

Easy to Use

If an organization has deployed Duo to protect their environment, Duo Trust Monitor doesn't require any additional deployment. The feature is maintained and tuned by the Duo team.

After deploying Duo, Duo Trust Monitor begins to ingest authentication logs to understand the access environment. It runs in the background, with no additional oversight required.

When flipped on, Duo Trust Monitor surfaces relevant security events in a simple, intuitive UI. Risk events can be easily exported into a favorite security information and event management (SIEM) tool via API. Trust Monitor is also integrated into the Cisco SecureX platform which consolidates threat intelligence across the network environment.

02

Detect Access Risk

Before Duo Trust Monitor, many organizations exported raw Duo authentication logs for analysis. Now, Duo Trust Monitor leverages machine learning to refine the logs based on historical and contextual patterns.

This rigorous analysis highlights cases where access is deemed highly anomalous or risky. For example, it may be expected that a user uses a personal laptop when travelling for work, but it is never expected that an engineer's credentials attempt access to HR applications from a new location.

To help organizations maintain awareness of their security posture and proactively remediate threats such as credential compromise, Trust Monitor sends email alerts when a new security event surfaces.

03

Improve Access Policy

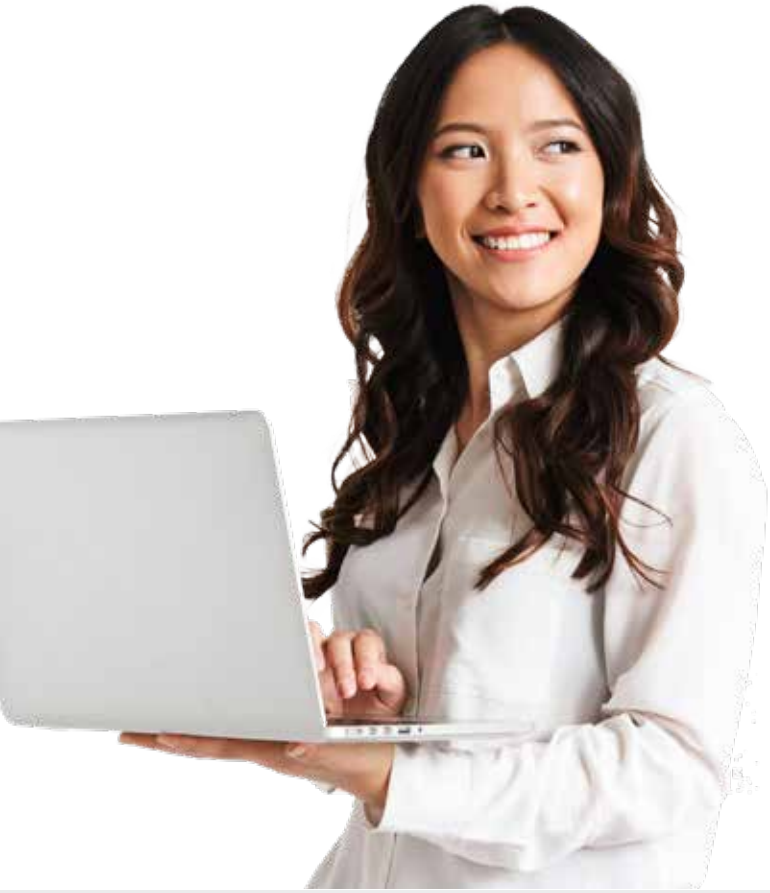
By highlighting cases of risky access, Duo Trust Monitor also surfaces areas where administrators may want to add or update access policy.

For example, let's say a user consistently uses Duo Push to authenticate into a highly-sensitive application. Then Duo Trust Monitor highlights a case where the user attempted to use SMS, a less secure factor, to authenticate. Depending on the company, this type of anomaly may inform a new policy stating that SMS isn't allowed as a factor for certain apps.

Without visibility into access patterns and anomalous activity, administrators miss a chance to harden defenses.

Duo Trust Monitor is a detection benefit many MFA solutions don't provide out of the box. For us, the highlighted risky events have been fairly spot on - with very few false positives."

– Jason Waits, CISO, Inductive Automation



CONCLUSION:

How is Duo Trust Monitor better?

Many access risk tools rely on overly simplistic rules like novelty alone (i.e. new location, new device). Simple rules have their place, but more often than not they lead to a slew of false positives. Setting off an alarm if an end user switches from a laptop to a phone adds needless friction if all other contextual variables like IP, location, and authentication method stay the same.

The algorithms employed by Duo Trust Monitor are explicitly tuned to Duo-specific data and targeted to reduce false positives by taking into account a holistic view of a user's authentication patterns. Over-the-counter, generic machine learning tools would be challenged to match Duo Trust Monitor's accuracy and precision.

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.

Cisco Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. A trusted partner to more than 40,000 customers globally, Duo quickly enables strong security while also improving user productivity.

Try it for free at duo.com.