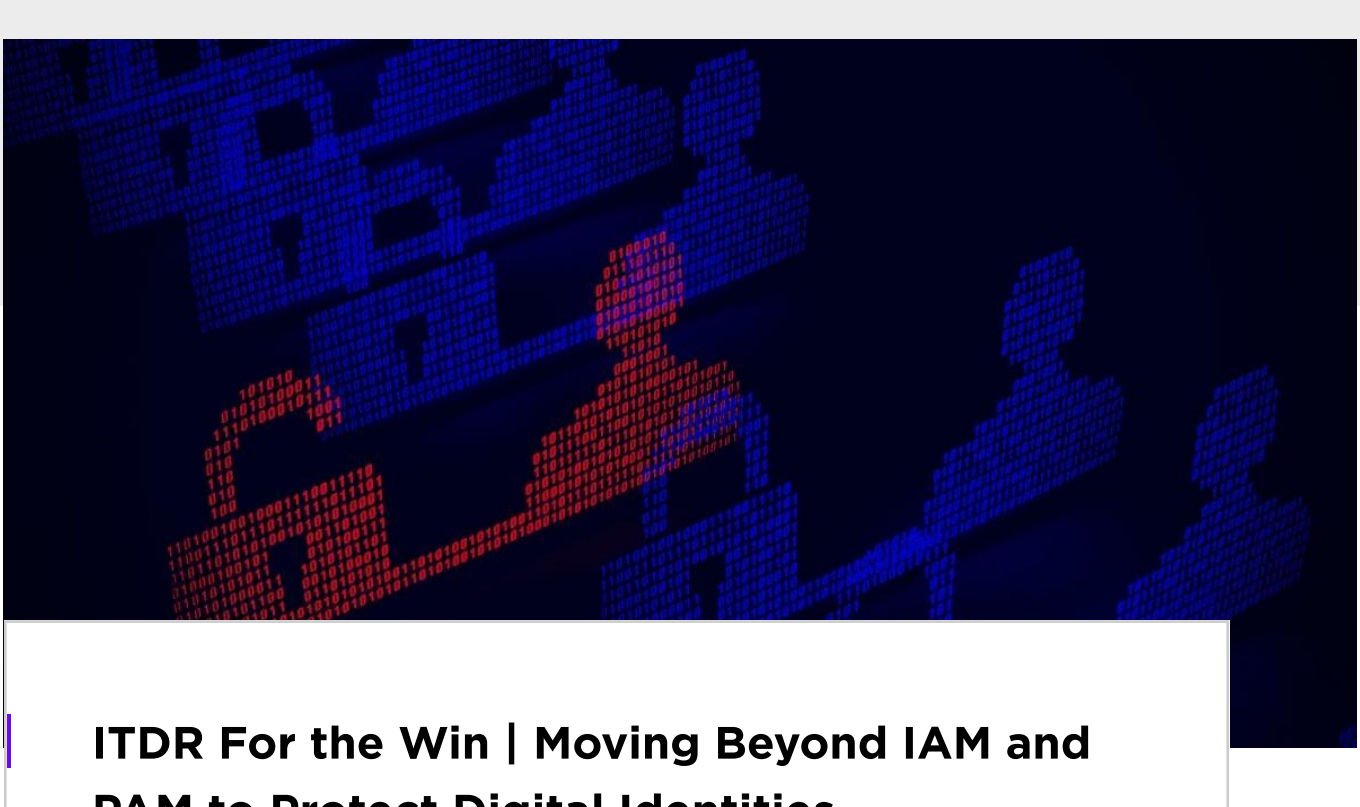


ITDR For the Win | Moving Beyond IAM and PAM to Protect Digital Identities

February 13, 2023
by SentinelOne

In today's modern work landscape, digital identities have become a record of trust, access, and relationship management for businesses. Regardless of their size and industry, organizations rely on digital identities to operate.

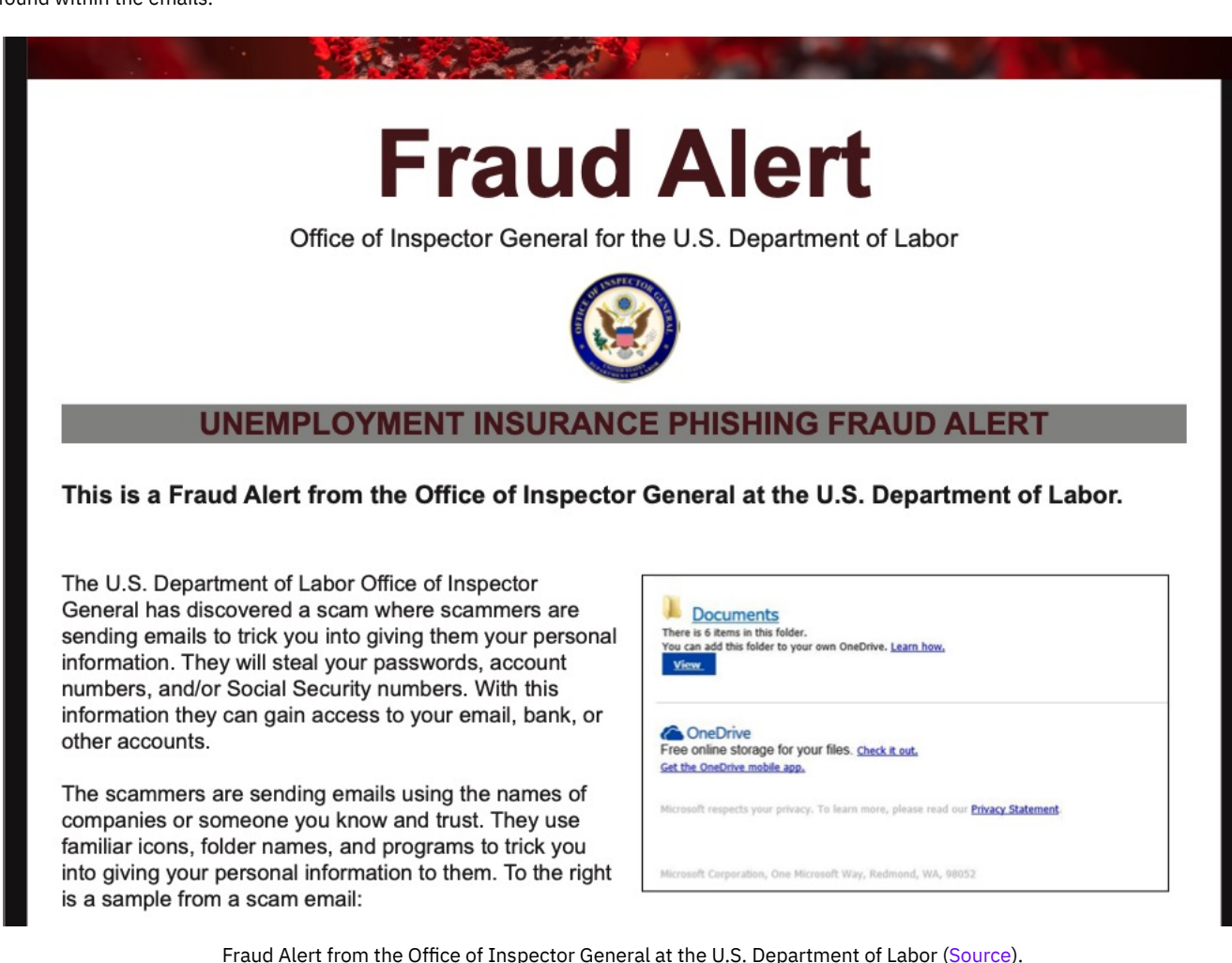
With a massive growth in the number of digital identities though, opportunistic threat actors have latched on to this expanding surface as a means for attack. Identity-based cyberattacks have accelerated and conventional identity management tools such as Identity Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) are no longer enough on their own to shield organizations from advancing cyber threats on both digital and machine identities.

Identity protection and management has increasingly become a topic of focus for many security leaders who now look towards a combination of identity threat detection and response (ITDR) strategies to reduce risk and protect the enterprise. In this post, we explore how ITDR can help protect against threat actors' growing interest in attacking identity and set up organizations for long-term success.

What Does the Threat Landscape Look Like for Identity?

Data leaks, phishing and social engineering campaigns, supply chain, and golden ticket attacks have all made global headlines over the past few years with, seemingly, no end in sight. Threat actors are after sensitive data and the volume of attacks on identity has grown significantly.

At the start of last year, for example, attackers impersonated the U.S. Department of Labor in a phishing campaign aimed at stealing Office 365 credentials. The emails asked recipients to submit bids and utilized an entire network of phishing sites to target unsuspecting users. This particular attack showed a high level of sophistication in the convincing setup of spoofed pages and the well-crafted, typo-free content found within the emails.



Fraud Alert

Office of Inspector General for the U.S. Department of Labor

UNEMPLOYMENT INSURANCE PHISHING FRAUD ALERT

This is a Fraud Alert from the Office of Inspector General at the U.S. Department of Labor.

The U.S. Department of Labor Office of Inspector General has discovered a scam where scammers are sending emails to trick you into giving them your personal information. They will steal your passwords, account numbers, and/or Social Security numbers. With this information they can gain access to your email, bank, or other accounts.

The scammers are sending emails using the names of companies or someone you know and trust. They use familiar icons, folder names, and programs to trick you into giving your personal information to them. To the right is a sample from a scam email:

Documents
There is 6 items in this folder.
You can add this folder to your own OneDrive. Learn how.
View

OneDrive
Free online storage for your files. Check it out.
Get the OneDrive mobile app.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation, One Microsoft Way, Redmond, WA, 98052

Fraud Alert from the Office of Inspector General at the U.S. Department of Labor (Source).

Later in 2022, authentication services provider Okta suffered a supply chain attack when a laptop belonging to a subprocessor support engineer was compromised. During the 5-day period of unauthorized access, the threat actors were able to access Okta's customer support panel and internal Slack server. The compromised account held 'super admin' access capable of initiating password resets of Okta's end customers.

Rounding up the tail end of 2022, multinational fintech company PayPal notified thousands of its users after their accounts and personal data were accessed by way of a credential stuffing attack. In this type of attack, threat actors rely on bots to pair massive lists of known usernames and passwords together to then 'stuff' into login portals. The breach impacted nearly 35,000 account holders with threat actors having accessed their full names, birthdays, mailing addresses, social security numbers, and tax identification numbers.

Identity-based attacks accounted for much of the reported security incidents from 2022. Attackers continue to exploit this attack surface, posing a direct risk to enterprises as they meet a surge in digital identities and remote workers.

Accelerated Attention on the Identity Attack Surface

The 2022 Trends in Security Digital Identities report from the Identity Defined Security Alliance (IDSA) noted the following key findings:

- 84% of respondents experienced an identity-related breach in the past year
- 96% reported that said breaches could have been minimized or even prevented by identity-focused solutions
- 78% reported direct business impacts such as reputational damage and the cost of recovery post-breach

The causes for this accelerated attention on identity can be attributed to two main factors.

First, the rising use of third-party technology and services, internet of things (IoT) connections, and cloud-based apps have all increased the number of digital identities – both human and machine. Each identity is another possible attack vector, and with so many in existence, more than a few are bound to be less protected or monitored as they should. Such low hanging fruit is a tantalizing 'in' for threat actors.

Second, securing new working spaces has become increasingly complex. The perimeters of work have extended far beyond physical offices or small numbers of off-site workers. Accelerated by a global pandemic, work-from-home policies have settled into many organization's very infrastructure. These allowances have also allowed vendors, partners, contractors, and third-party service providers to all remotely access network resources as needed.

Understanding the Growing Digital Identity Crisis

Digital identities for both humans and machines are an integral part of how we operate on a day-to-day basis. Vulnerable to attackers, what's emerged is a high-stakes digital identity crisis that affects everyone. Top challenges businesses face in securing digital identities include:

- A lack of investment for identity management systems – Cloud-based identity architectures are enjoying a boom in adoption, but many small to medium-sized businesses still show resistance to migrating due to budgetary constraints, concerns about onboarding delays, lack of change management processes, and more.
- Fractured ownership for identity in many organizations – Identity management and security is often a responsibility divided amongst the executive leadership and multiple teams like IT, human resources, or sales, for example.
- Fluctuating data privacy regulations and controls – Digital identity management is made complex by the moving goal posts issued by regulatory bodies. Inevitably, identity and data privacy overlap, so organizational leaders must ensure that the data surrounding digital identities comply with mandates such as the European Union's GDPR, the NIST Privacy Framework, ISO/IEC 27701:2019, and the Personal Information Protection and Electronic Documents Act (PIPEDA).

> While organizations contend with the above challenges, the task of securing digital identity lags behind new threats and many traditional means of protection are no longer able to meet developing attack vectors head on.

Password-based authentication systems, for example, are well known for the inherent risks they bring. Hackers can employ brute force, password spraying, and credential stuffing attacks on these systems to steal passwords. Organizations that don't design and enforce strict password hygiene processes are vulnerable to user-generated threats stemming from the recycling of the same passwords across multiple accounts, forgetting passwords, and storing passwords in unsafe places.

Threat groups also target unsecured cloud users via cloud solution providers (CSPs) through credential theft techniques, phishing attacks, and conducting malicious activities to obtain usernames and passwords.

Legacy multi-factor authentication (MFA) protocols have also come under attack with threat actors targeting a number of big names in 2022 alone, among them Twilio/Okta, Microsoft Teams, Dropbox, and Cisco. While MFA is a commonly recommended and good security best practice, it is only as strong as its weakest link and implementing it alone is not sufficient to protect organizations from identity-based attacks.

In understanding the growing digital identity crisis, security leaders recognize the dire need for robust identity management solutions that combine proactive endpoint defense, real-time and managed response, zero-trust infrastructure, and domain protection.

Understanding the Limitations of Legacy Identity Management Tools

Existing identity protection solutions such as Identity Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) generally focus on making sure people have access to only what they need. Authorization and authentication are the main pillars covered by these types of solutions, but they are unable to provide visibility into key factors in identity breaches: credential misuse, exposures, and privilege escalation activities from the endpoint into cloud and Active Directory (AD) environments.

Security for identities isn't only managing user access, policing governance, or locking down exclusive privileges – organizations are now looking to assess security gaps from an identity standpoint. This means proactively looking at root causes and thwarting identity-based threats before they become full scale security events.

Since identity is one of the most attacked perimeters enterprises now face, the importance of looking beyond simply managing access and moving towards a proactive defense of the entire infrastructure has come to the fore. Threat detection solutions can be geared specifically towards identity-related indicators of compromise, stopping threat actors before they can gain unauthorized access or raise their privileges in a victim's network.

How ITDR Sets Up an Organization for Success

To secure the infrastructure in which identities are managed and used, identity threat detection and response (ITDR) has come to the forefront as an adjacent framework to advanced security solutions like Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR). ITDR works to fill a significant gap in the threat landscape, focusing on protecting credentials, privileges, cloud entitlements, and all the systems that manage them.

With ITDR in place, organizations are set up to:

- Proactively detect and prevent identity-based threats – ITDR actively looks for attacks targeting identity vectors, detecting credential theft, signs of privilege misuse, and malicious actions on AD. Singularity™ Hologram, for example, can detect phishing attacks targeting victim identity information.
- Thwart attack progression – ITDR solutions add an additional layer of protection in an environment by redirecting attackers to pre-set decoys, automatically isolating affected systems, and stopping them from moving laterally into other networks. Singularity™ Identity detects advanced attack techniques that threat actors use to move laterally inside an organization's network, data center, cloud environment, remote site, or branch offices.
- Build long-term cyber resilience – ITDR brings value to forensic data collection as it gathers key telemetry on processes used in attacks. Collected threat intelligence can be used by technical teams to strengthen weak policies and processes.
- Extend protection to cloud environments – Clouds can often encourage permissions sprawl, overwhelming many teams with too many applications, containers, and servers to manage. ITDR solutions extend to cloud environments by delivering visibility into risky entitlements that may give way to opportunistic attackers.

Conclusion

As identity-based threats continue to strike across all global industries, business leaders are doubling down on reducing risk during a digital identity crisis. Organizations can move towards cybersecurity strategies and solutions with identity protection at its center to ensure protection against mounting attacks, manage machine and user identities at scale, meet regulatory compliance needs, and build client trust.

Digital identities are the foundation of many organizations and SentinelOne's Identity Suite delivers robust defenses to defend the infrastructure that houses them. Whether organizations are on-prem or in the cloud, Singularity ends credential misuse through deception-based protections executed in real-time.

Learn more about how Singularity furthers identity-leading cybersecurity strategies by booking a demo or visiting Singularity™ Identity.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Detecting Unconstrained Delegation Exposures in AD Environment
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- Top 10 Ways to Protect Your Active Directory
- Detecting a Rogue Domain Controller – DCShadow Attack
- Protecting Your Active Directory from AdminSDHolder Attacks
- Rise in Identity-Based Attacks Drives Demand for a New Security Approach