protiviti®

Face the Future with Confidence

Towards an

Identity-Centric Security Strategy

Internal Audit, Risk, Business & Technology Consulting

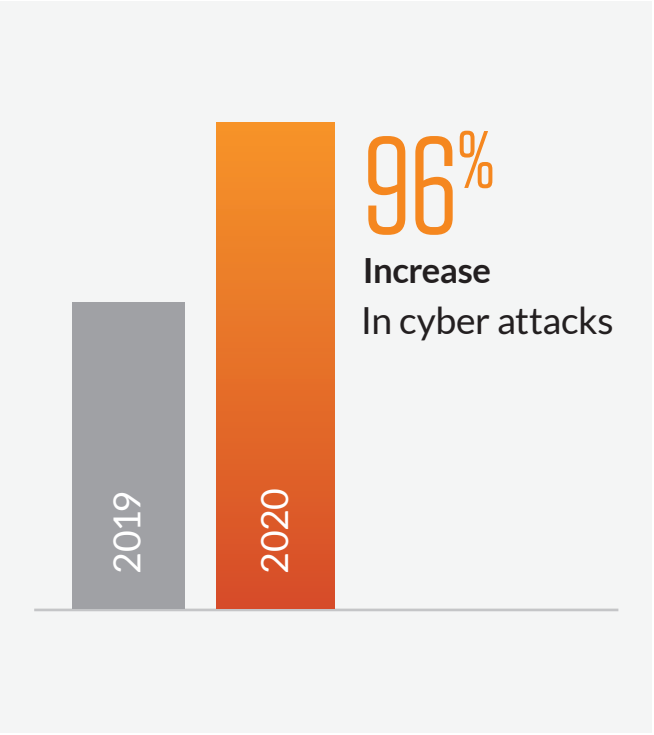
Cyber attacks are rampant

Let's face it, cyber security professionals are not faring well against the increasing sophistication of attacks by hackers.

According to the 2020 Verizon Data Breach Investigations report, the world witnessed a challenging year with a whopping 96% increase in successful data breaches against U.S. companies and government agencies as compared to 2019.

Cyber attacks have now played a role not only in criminal endeavours but international politics as well.

What are we missing?



Source:

Verizon DBIR 2019: 96% increase of successful breaches from 2019 to 2020 (2,013 to 3,950, respectively)

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

It's not (just) a budget or staffing issue

Unfortunately, the solution isn't a simple increase in security budgets, though that has certainly been tried in spades. In fact, worldwide spending on security-related hardware, software, and services was an estimated $125.2 billion in 2020, an increase of 6% over 2019, according to researcher IDC. And that number is expected to reach $174.7 billion in 2024, with much of it dedicated to the elements of the "security stack" listed in the sidebar.

Even with all of the additional spending, 2020 was a record year for data breaches, including the high-profile compromises at Microsoft and Facebook. 3,950 data breaches compromised more than 36 billion records, shattering previous all-time records

In order to understand why all this technology and human capital investment is still not staunching the flow of successful attacks, we need to understand how most of those attacks happen in the first place.

The security stack

- **UBA**: User behaviour analytics
- **IGA**: Identity governance & administration
- **PAM**: Privileged access management
- **CASB**: Cloud access security broker
- **EMM**: Enterprise mobility management firewalls / network
- **VPN**: Virtual private network
- **DLP**: Data leakage prevention

Source:

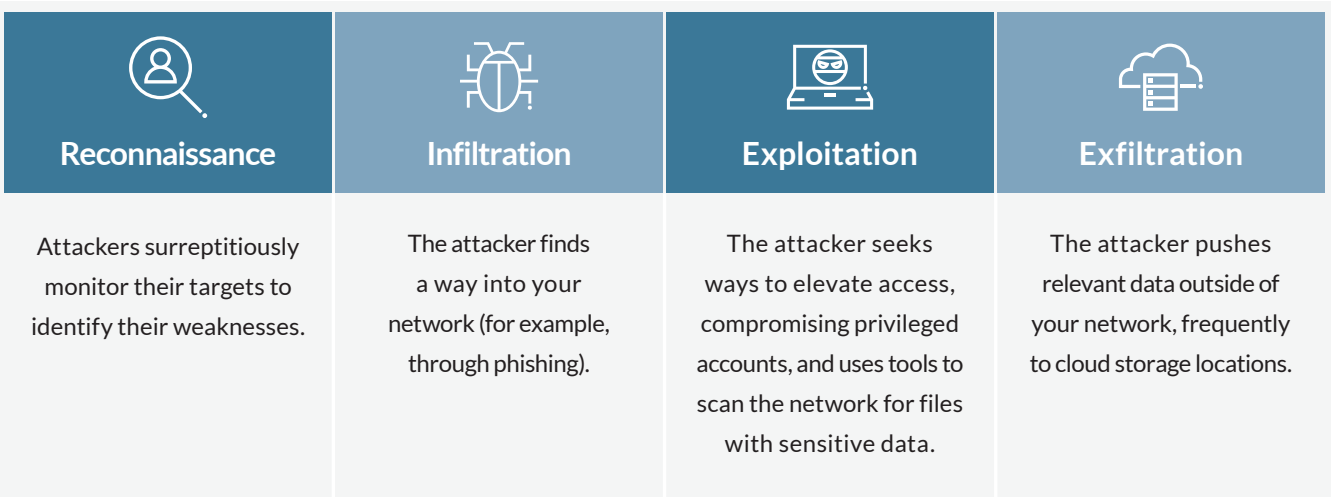
Security Magazine: Top 10 Data Breaches of 2020 (including Microsoft and Facebook)
https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020

International Data Corporation (IDC): Security-related hardware, software, and services spend was an estimated $125.2 billion in 2020, an increase of 6.0% over 2019
https://www.idc.com/getdoc.jsp?containerId=prUS46773220#:~:text=According%20to%20a%20new%20forecast,increase%20of%206.0%25%20over%202019.

Infosecurity Magazine: 2020 breaches comprise of more than 36 billion records.
https://www.infosecurity-magazine.com/news/number-of-breached-records-hits-36/

The anatomy of a data breach

Generally, a data breach follows the same pattern, typically referred to as a "Kill Chain", and occurs in 4 steps:



A careful reader will notice an interesting fact: Most organisations today already have most, if not all, of the tools that they need to detect and correct each step in the kill chain (see sidebar on previous page). However, in spite of having these tools in their arsenal, those organisations still remain vulnerable to breaches.

Source:

This model was proposed by SailPoint CTO Darran Rolls, and is itself a condensed version of a seven-step model originally forwarded by Lockheed-Martin circa 2013

Mind the gap

An organisation has many types of internal controls, of which two important ones are detective controls and corrective controls. As their names imply, detective controls are responsible for noticing signs of bad activity, and corrective controls are the mechanisms by which that bad activity can be stopped in its tracks. Most elements of an organisation's "security stack" serve as either detective controls or corrective controls, and some do both.

The challenge is that most of the detective and corrective components in an organisation's security stack are not well integrated. Even though all of your company's controls may be working as designed, they're not communicating with one another, creating gaps in coverage and delays in response times. Sophisticated attackers exploit these gaps and delays to proliferate within your network and exfiltrate your data.

A new approach is needed to effectively defend against modern cyber attacks. Central to this approach is the notion that these various crucial elements of an organisation's security arsenal need to be integrated and work together in a well-orchestrated and unified manner.

Identity at the centre

Identity can unify your cyber security strategy in a meaningful way. It is the central and common construct that threads through your entire security and IT infrastructure.

Analysis of the anatomy of the data breach points to a glaring fact: there's a direct relationship between the quality of an organisation's controls of their digital identities and the strength of its ability to successfully defend against breaches.

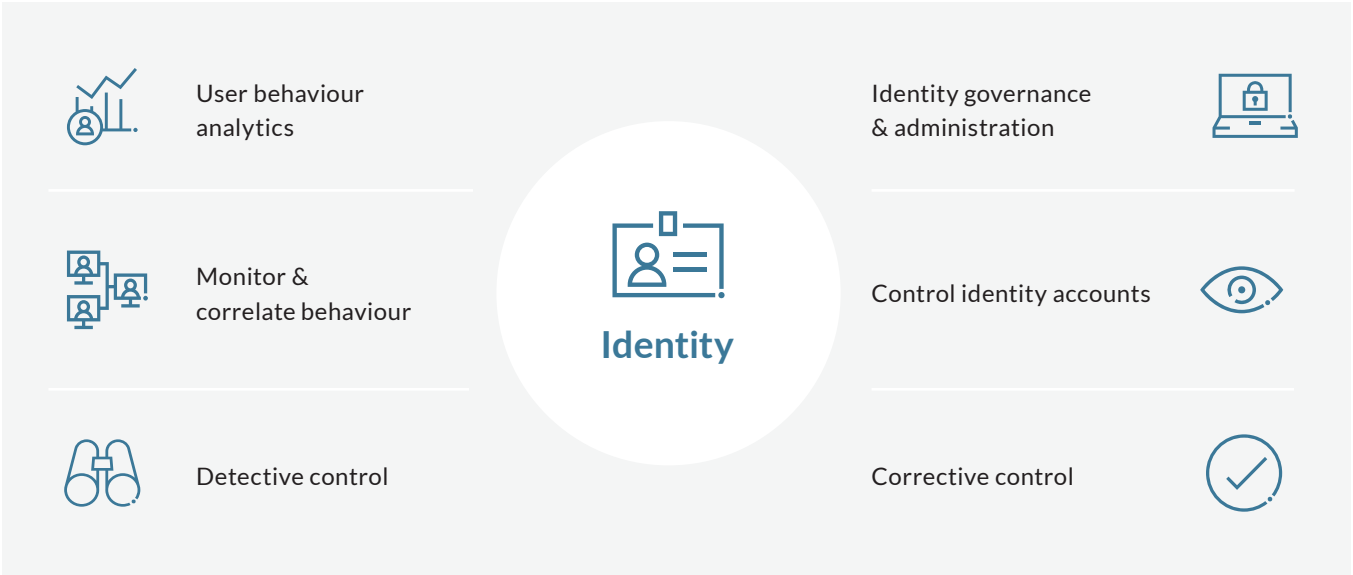
Steps 1, 3, and 4 of the Kill Chain can be identified based on patterns of identity behaviour (what identities are doing), and steps 2 and 3 rely on compromising identity accounts (what identities have access to). When compromised, this combination can launch a devastating attack on an organisation's data and resources.

Therefore, identity-related technologies must be at the core of an organisation's security architecture — specifically, technology that controls both an organisation's identity accounts and identity behaviour. Luckily, technologies already exist that provide effective controls for both aspects of digital identity.

User Behaviour Analytics (UBA) refers to the evolution of security intelligence and event management (SIEM) platforms towards an identity-centric paradigm. Using pre-defined rules as well as AI and machine learning, a UBA solution understands normal behaviour patterns for a user or groups of users and can then warn an organisation when a user is behaving abnormally.

Identity Governance & Administration (IGA) platforms bind users to the various accounts that they can access. They are the foundation of a broader identity management process that ensures that accounts and privileges are properly managed in line with a given user's roles and responsibilities within their organisation.

UBA can form the foundation for an organisation's detective controls — those controls that are responsible for catching signs of bad activity. Conversely, IGA for the most part delivers corrective controls — the mechanisms by which bad activity can be stopped in its tracks.



Identity as the foundation for detective controls

Identity technologies can provide a robust detective control layer for the enterprise. The following chart illustrates some of the detective capabilities of identity technologies.

Reconnaissance

Infiltration: UBA technology can identify abnormal behaviour, such as a log in from a new endpoint. Or repeated authentication attempts. Or geographically dispersed authentication attempts. It can even address more complex scenarios, such as, "identify all sessions where the user came in via the VPN from a new country for the first time, then created a new account, then accessed a server for the first time, and then malware was detected on that server."

Exploitation: IGA technology can share the complete list of accounts associated with an identity with UBA, thereby enabling UBA with the ability to track user behaviours across sessions.

UBA technology can detect when a user attempts to switch accounts to a high-privileged account for the first time.Privileged User Management technology can share the list of high-privileged accounts with UBA.

UBA technology can also flag abnormal behaviour, such as scanning that typically occurs as part of a data breach.

Exfiltration: UBA technology can identify behaviour that is indicative of exfiltration including unusual patterns of data uploads to cloud repositories and emailing abnormally high volumes of sensitive data in the form of attachments.

Breaking the kill chain: Integrating detective and corrective controls

As shown previously, an identity-centric foundation can provide detective controls at each phase of a data breach. But detection alone only alerts security administrators of danger — and although that is valuable in and of itself, policy-based integration amongst security products can go a long way in automating technologies that provide corrective controls.

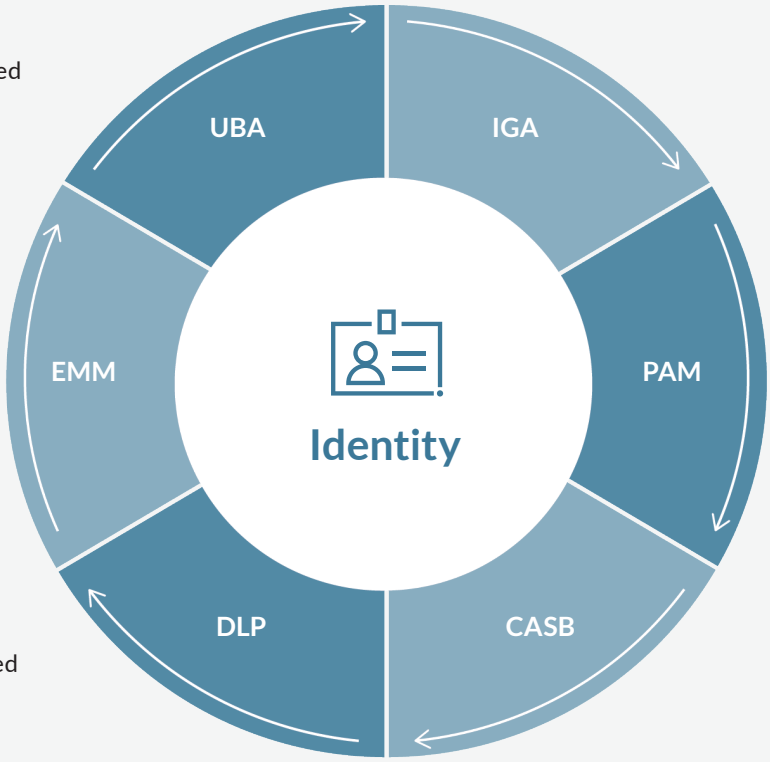
Most enterprise security organisations have an extensive array of cyber security software that provide a rich layer of corrective controls. Unfortunately, such controls are worthless unless triggered at the appropriate time. With a combination of finely tuned detective controls, and the real-time invocation of corrective controls, you can create a powerful cyber defence to help you thwart data breaches.

01

UBA
Triggers alert based on bad behaviour

02

IGA
Automatically takes corrective action in AD, HR, finance, and other systems.



04

Identity Data
Continues to be fed back into UBA to improve baseline

03

PAM, CASB, DLP, EMM, etc.
Take additional corrective action based on trigger from UBA or IGA

Identity-centric cyber security in action

Let's examine two common scenarios to better understand how an identity-centric security architecture empowers an organisation to better defend itself against cyber attacks.

Scenario 1:

Infiltration via Brute Force

Brute force attacks are a common way for a hacker to infiltrate your company. They're relatively cheap and can be executed quickly and effectively with the tools that are available today. In many cases, these types of attacks go initially unnoticed, are typically attributed to user error, and are not discovered until far too late.

The IGA platform identifies repeated failed login attempts from an unknown IP address. The UBA further correlates that this IP address has had numerous failed login attempts across multiple accounts, denoting a potential attack.

With an identity-centric architecture, the following actions can be taken immediately and without human intervention:

- Automatically configure the firewall to refuse connections from that IP address.
- Route the traffic to a honeypot for further analysis.
- Automatically lock the accounts that are being attacked and force a password change action for those users.
- Notify the users that there is suspicious activity on their account.
- Prompt a step-up authentication to challenge those users to provide additional information or security token before authenticating.
- Notify the security team of a possible breach attempt.

Scenario 2:

Data exfiltration

A privileged identity is invoked for the first time. In isolation, this is only a mildly suspicious action. The user identity's risk score is incremented to a level of "alert".

A short time later, a different user identity initiates an unusual file transfer that is a variance from the norm for this identity, based on the file size, file type, and the timeframe when that activity is taking place. This also raises that user's risk score to a level of "alert".

Because IGA has bootstrapped UBA with a mapping of human users with privileged accounts, the UBA system now knows that both these alerts were tripped by the same user. The UBA correlation and analytics engine determines that both these actions taken together constitute a potential threat, raising the risk score to "critical".

Because the company's security architecture is well integrated, the following actions are immediately taken in real time and without human intervention:

- IGA is alerted that the identities associated with the event should be disabled immediately using automated deprovisioning events where possible (for example the AD account).
- The VPN system is alerted to block the IP address that was associated with the suspicious activities.
- The DLP system is alerted to block further file transfers or emails from the identities involved (in case the identities have active sessions on these systems).
- CASB and EMM are notified to immediately block all access for that user from mobile devices and to any cloud assets.
- Security personnel are alerted to investigate the potential incident and all data related to all of these activities is logged for forensic analysis.

Conclusion

Cyber security is more challenging now than it has ever been before. Fortunately, there's a veritable arsenal of sophisticated tools that you have at your disposal to stay ahead of the enemy. However, most organisations are not yet using those tools in a smoothly orchestrated and integrated manner.

Identity is the common element that threads through your IT and security infrastructure, and can serve as the unifying construct to synchronise your defences.

Using identity to integrate UBA-driven detection tools and IGA-driven enforcement tools, you can take an adaptive and responsive approach to cyber security and significantly improve the security posture of your organisation.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®