# defending against advanced persistent threats: strategies for a new era of attacks

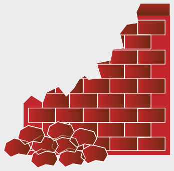
agility
made possible™

ca®
technologies

# security threats as we know them are changing

The traditional dangers IT security teams have been facing – and overcoming – for years are being replaced by a far more hazardous, insidious form of attack: the Advanced Persistent Threat (APT).

Although APTs are an emerging threat vector, their impact has already been felt in substantial ways:



## RSA SecurID Hack

In 2011, an APT compromised the systems containing information about RSA SecurID two-factor authentication tokens, including the values the company uses to generate one-time passwords.[1]

## Operation Aurora

Hackers stole sensitive intellectual property, including source code, from Google, Adobe, and other high-profile companies using highly sophisticated, well-coordinated techniques.[2]

The financial impact of an APT cannot be underestimated:

On average, it costs organizations

**$5.5 MILLION**

to respond to and address the aftermath of an APT attack.[3]

[1] PCWorld. "RSA SecurID Hack Shows Danger of APTs." March 18, 2011.
[2] Wired. "Google Hack Attack was Ultra Sophisticated, New Details Show." January 14, 2010.
[3] Ponemon Institute. "2011 Cost of Data Breach Study." 2011

# what makes an APT an APT?

An APT is a long-term, sophisticated strike launched against a specific, targeted entity. By its very definition, an APT is not your "normal" threat:

**ADVANCED:** The attacker has the significant technical capabilities required to take advantage of weaknesses in the target – including coding skills and the ability to uncover and exploit previously unknown vulnerabilities.

**PERSISTENT:** Unlike short-term, one-off hacks that capitalize on temporary opportunities, APTs often unfold over the course of years, employ multiple vectors and combine security breaches over time to gain access to more – and significant – data.

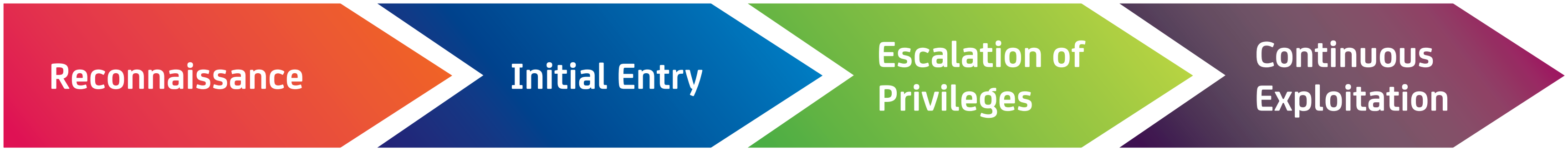
**THREAT:** The individuals, groups and organizations that execute APTs have the motivation, ability and resources needed to be successful.

APT perpetrators are often state-sponsored entities with objectives that reach far beyond simple theft. These include:

- Military Intelligence
- Economic Sabotage
- Technical Espionage
- Financial Extortion
- Political Manipulation

# how an APT works

Nearly every APT follows four phases:



Reconnaissance

Initial Entry

Escalation of Privileges

Continuous Exploitation

**1**

An investigation into the organization's weaknesses, which often includes domain queries and port and vulnerability scans.

**2**

Discovered exposures are exploited and a foothold in the target network is established using sophisticated technical methods or social engineering techniques, such as spear phishing.

**3**

Following initial penetration, hackers work to acquire more rights and gain control over additional systems – and install a "back door" that makes future access easier.

**4**

Once control has been established, the assailant will be able to continuously identify, compromise and exploit sensitive data.

And since the third and fourth stages often occur over a matter of years, detecting an APT can be incredibly difficult.

# traditional security is no match for an APT

Targeted threats, highly advanced methods and well-funded, motivated perpetrators make standard Internet and network security measures an insufficient defense against APTs. While common perimeter and infrastructure protection may help prevent or delay the initial network penetration, they can do little once a foothold has been established.

For these reasons, organizations require a more proactive, comprehensive protection strategy – one that can detect APTs earlier and prevent attempts to escalate privileges or export sensitive data.

## Why do the traditional rules of Internet security no longer apply in the world of APTs?

- Patient individuals will wait for new vulnerabilities to open up or combine seemingly small techniques into a large-scale, damaging attack
- A dedicated, state-sponsored enemy will not be dissuaded from targeting an organization simply because it has stronger security than similar companies
- An APT can unfold in a very measured, deliberate manner, helping it evade even the most well-configured firewalls and intrusion-detection systems

# defense-in-depth is the key to stopping APTs

Successful protection against APTs should complement traditional perimeter and infrastructure security measures, so the organization is able to:

- Make the initial penetration difficult
- Reduce the potential for privilege escalation in the event an account is compromised
- Limit the damage that can be done by a compromised account
- Detect suspicious activity early in the intrusion attempt
- Gather the information forensic investigators need to determine what damage occurred, when and by whom

What's needed, then, is "defense-in-depth," a strategy that complements traditional security solutions with such identity and access management capabilities as:

shared account management

virtualization security

least privilege access

identity management and governance

session recording

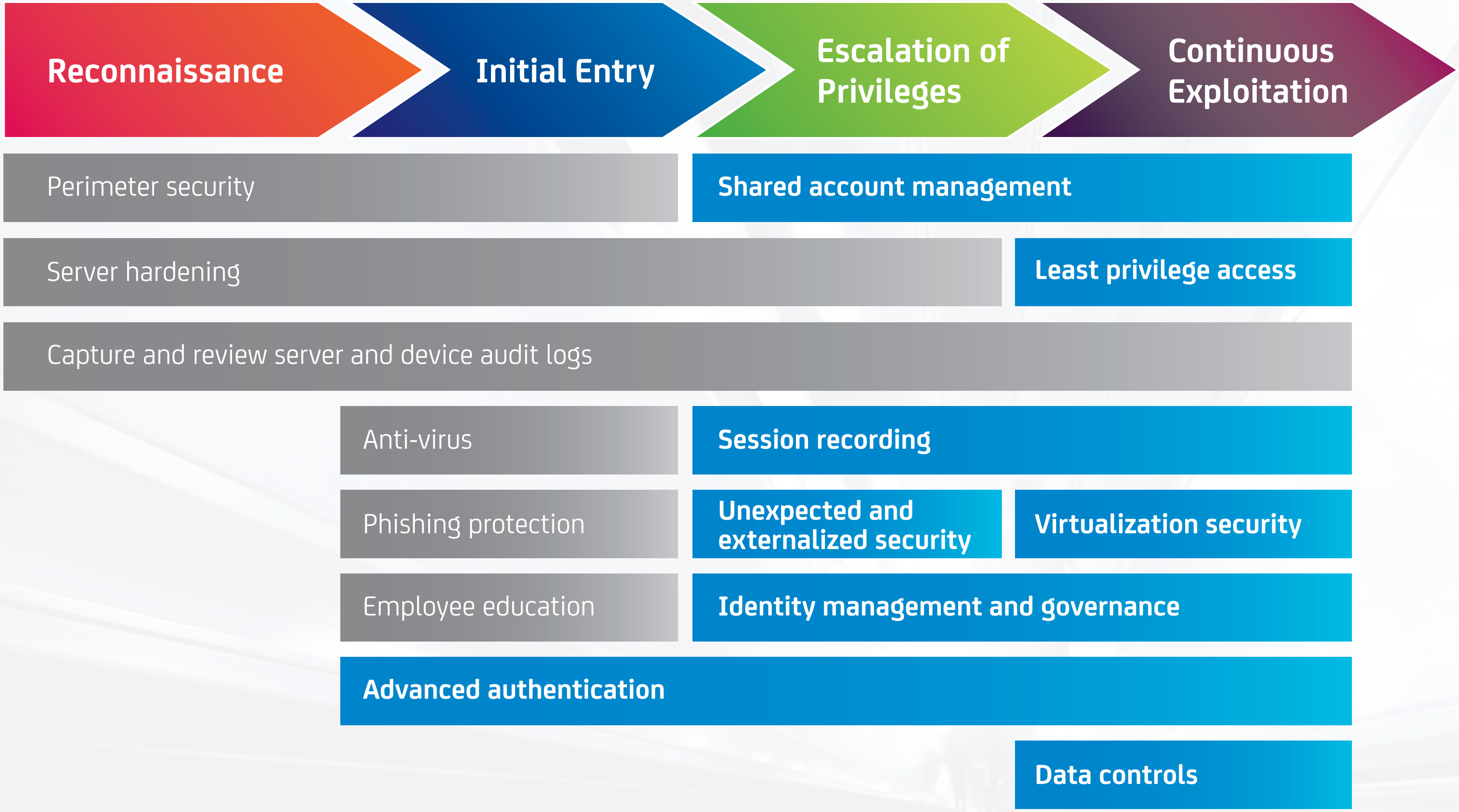
advanced authentication

server hardening

data controls

unexpected and externalized security

A defense-in-depth strategy extends traditional perimeter and system security with identity and access management tools, providing protection against APTs across all four phases of the attack.



Reconnaissance

Initial Entry

Escalation of Privileges

Continuous Exploitation

Perimeter security

Shared account management

Server hardening

Least privilege access

Capture and review server and device audit logs

Anti-virus

Session recording

Phishing protection

Unexpected and externalized security

Virtualization security

Employee education

Identity management and governance

Advanced authentication

Data controls

# defense-in-depth at a glance

**shared account management**

**least privilege access**

session recording

server hardening

unexpected and externalized security

virtualization security

identity management and governance

advanced authentication

data controls

## shared account management

Accessing and exploiting privileged accounts is a key tactic in all APT attacks. For this reason, shared account management capabilities should be able to:

- Securely store encrypted passwords
- Manage password complexity and make automated changes according to policy
- Restrict access to administrative accounts
- Prevent password sharing by using automatic login capabilities
- Limit the number of people who have access to privileged accounts by providing emergency account access
- Eliminate the use of hard-coded passwords in scripts

## least privilege access

Access should not be treated as an “all or nothing” decision. Instead, individuals should be given the credentials required to accomplish their assigned tasks. For example:

- **System administrators** should be allowed to update server software, make configuration changes and install new software – but shouldn’t be free to change security settings or view logs
- **Security administrators** should be able to update and alter settings and configurations and view log files – but shouldn’t be permitted to install software or access sensitive data
- **Auditors** must be able to check security settings and view log files – but shouldn’t be allowed to make any changes to a given system

# defense-in-depth at a glance

continued

shared account management

least privilege access

**session recording**

**server hardening**

unexpected and externalized security

virtualization security

identity management and governance

advanced authentication

data controls

## session recording

Tracking what actions are being performed by privileged accounts is a critical step in detecting APTs. To this end, session recording must be able to:

- Visually show “who did what”
- Provide analytical tools that expedite breach investigations by eliminating the need to look through gigabytes of hard-to-read text file logs
- Track the time, date, source IP and user ID of all logins
- Note any commands the user enters
- Connect anomalous behavior with the individual who performed it

## server hardening

Any server that hosts sensitive information must be configured in a way that protects it from being compromised by an APT. This should include:

- Using a firewall to control communications, restrict packets and block unsecure protocols
- Employing application whitelisting to allow only explicitly specified executions and installations
- Defining a specific set of actions for high-risk applications
- Preventing changes to log files
- Monitoring the integrity of key files
- Controlling access to directory files

# defense-in-depth at a glance

continued

shared account management

least privilege access

session recording

server hardening

**unexpected and externalized security**

**virtualization security**

**identity management and governance**

advanced authentication

data controls

## unexpected and externalized security

Individuals who launch APTs often use common operating system commands, functions and utilities to their benefit. These techniques can actually aid in the defense against APTs by:

- Using external tools to monitor and protect files, so they appear unsecured but actually allow administrators to detect an attacker's attempts to compromise the network
- Modifying the name of common system commands, so any use of the original triggers an alert

## virtualization security

The number of virtualized systems has skyrocketed, making these environments – and the hypervisor in particular – key targets of APTs. To protect virtual infrastructures, organizations should:

- Apply the principle of least privilege to hypervisor accounts
- Monitor and log all actions that occur at the hypervisor layer
- Secure virtual machines by leveraging virtualization-aware automation capabilities

## identity management and governance

Carefully protecting user identities is an essential step in minimizing the effectiveness of an APT attack. To this end, identity management and governance functionality must be able to:

- De-provision and de-authorize identities as soon as an individual leaves the company
- Find and remove orphaned, or unused, identities

# defense-in-depth at a glance

continued

shared account management

least privilege access

session recording

server hardening

unexpected and externalized security

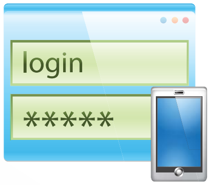
virtualization security

identity management and governance

**advanced authentication**

**data controls**

## advanced authentication



Two-factor authentication and risk-based evaluations help to protect against the initial penetration of an APT by denying or detecting inappropriate access attempts. To be as effective as possible, advanced authentication capabilities should include:

- Software-based, two-factor credentials that vary by device
- Versatile authentication methods that can be matched to a specific scenario
- Rules that adjust to protect against different APT tactics
- Device identification, geolocation, IP blacklisting and case management for suspicious activities
- The ability to step up authentication when stronger identity assurance is required

## data controls

Since the end goal of any APT is to steal sensitive information, having firm control over this data is a core component of a successful defense. To safeguard these assets, data must be:

- Classified according to sensitivity and type – at access, in use, in motion, at rest, etc.
- Controlled as it is transferred between sources, such as email and physical drives

# a holistic approach to security reduces risk

The concept of defense-in-depth is an essential component of any proactive, holistic APT protection strategy. The techniques supporting this approach work in concert to enable you to build and apply a security model that allows or denies actions based on business rules, data sensitivity and specific types of behavior.

Because this model can be applied uniformly across platforms and separated from operating system security, it provides an effective means of preventing and detecting APTs. As such, defense in-depth helps your organization stay one step ahead of APTs and reduce the effects such an attack can have on the business and its employees, customers and partners.

# about the solutions from CA Technologies

CA security solutions are comprised of a broad, comprehensive and integrated suite of capabilities that simplifies operations and reduces the total cost of management across cloud, on-premise, virtual, physical, distributed and mainframe environments – helping you significantly increase business agility.

Unlike traditional solutions, the CA suite controls not only user identities and the availability of critical IT resources, but also access to sensitive information assets. This provides more layers of security than conventional solutions – and helps to reduce the risk of breaches, minimize information loss and simplify compliance audits.

These offerings are complemented by a range of cloud-based identity services, which give you the flexibility to deploy security services how and when you choose, so you can adopt cloud or hybrid models in a way that fits your unique needs.

The CA Identity and Access Management suite covers the following areas:

- Identity Management and Governance
- Privileged Identity Management and Virtualization Security
- Advanced Authentication
- Data Protection
- Cloud Security
- Secure Single Sign-On and Access Management

CA Technologies (NASDAQ: CA) is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 relies on CA Technologies to manage evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

ca®
technologies