How Endpoint Detection and Response (EDR) Can Help Stop Breaches

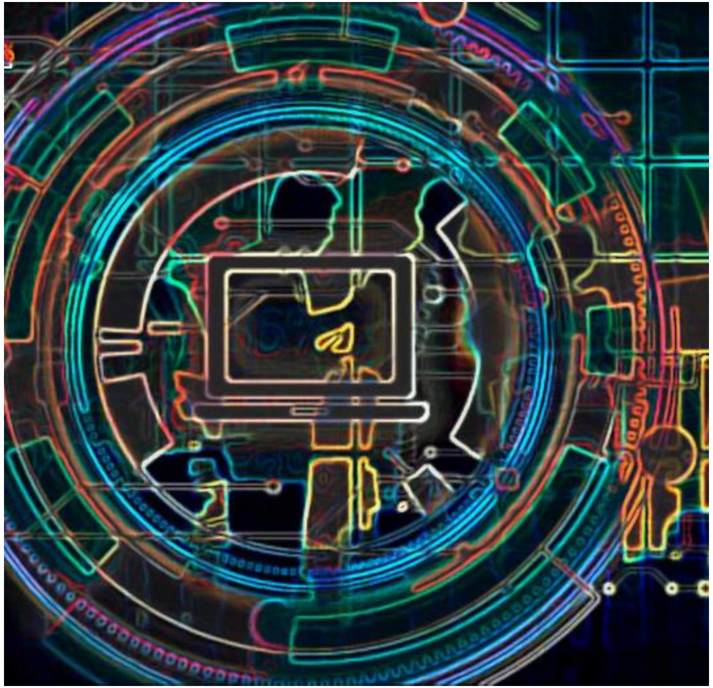
May 24, 2022

Scott Dale

Manager, Technical Product Management – Jack Henry

What we'll cover

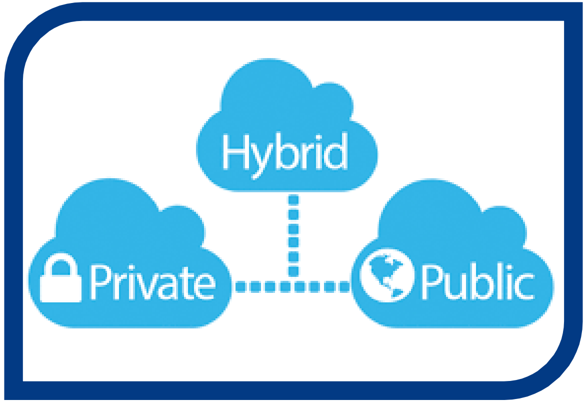
- Today's Threat Landscape
- What is EDR
- Best Practices
- Key Takeaways



Today’s Banking Security Dilemma

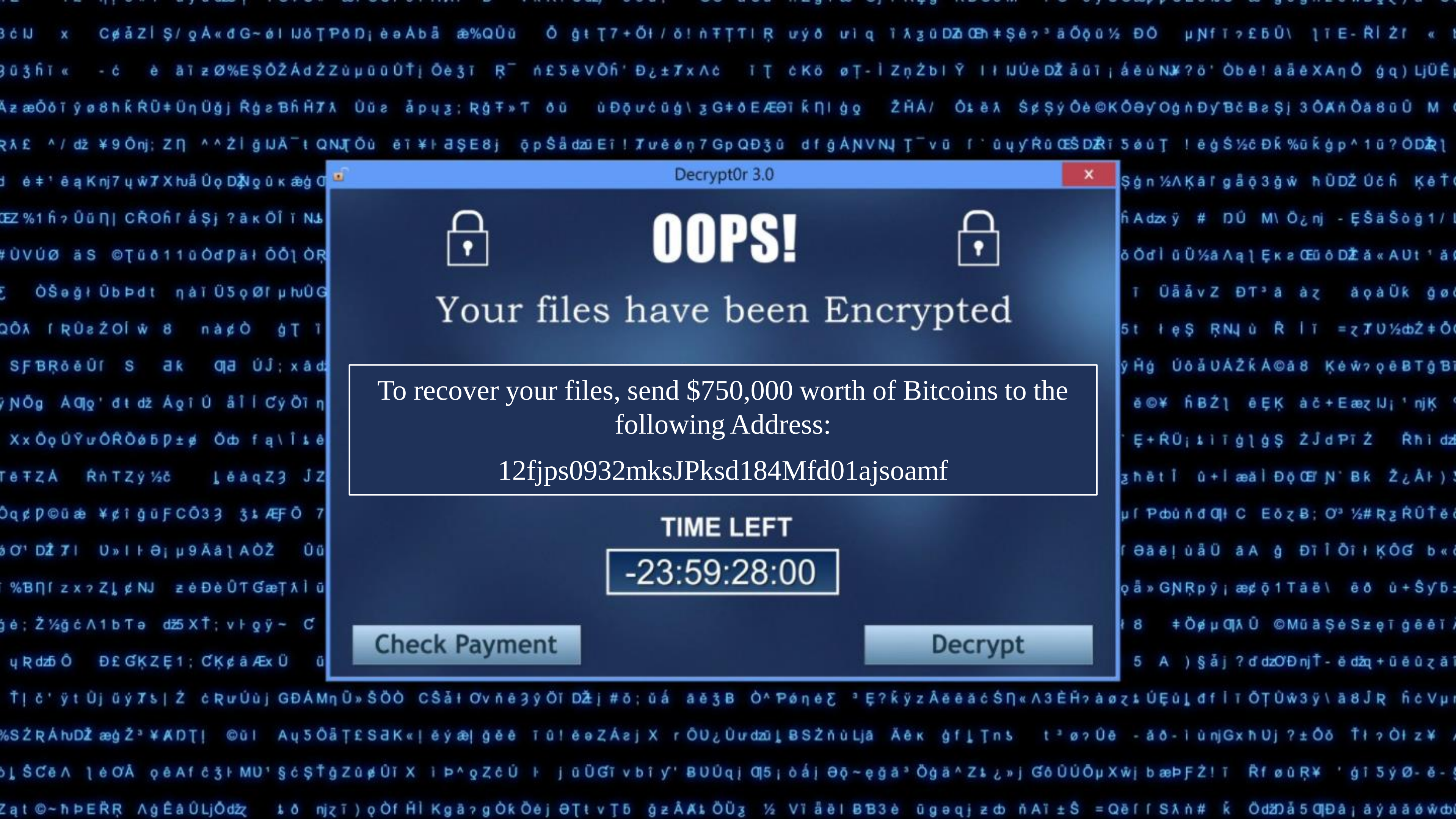
Sophisticated Threats

Complex Environments



Resources

ZERO DAY



OOPS!

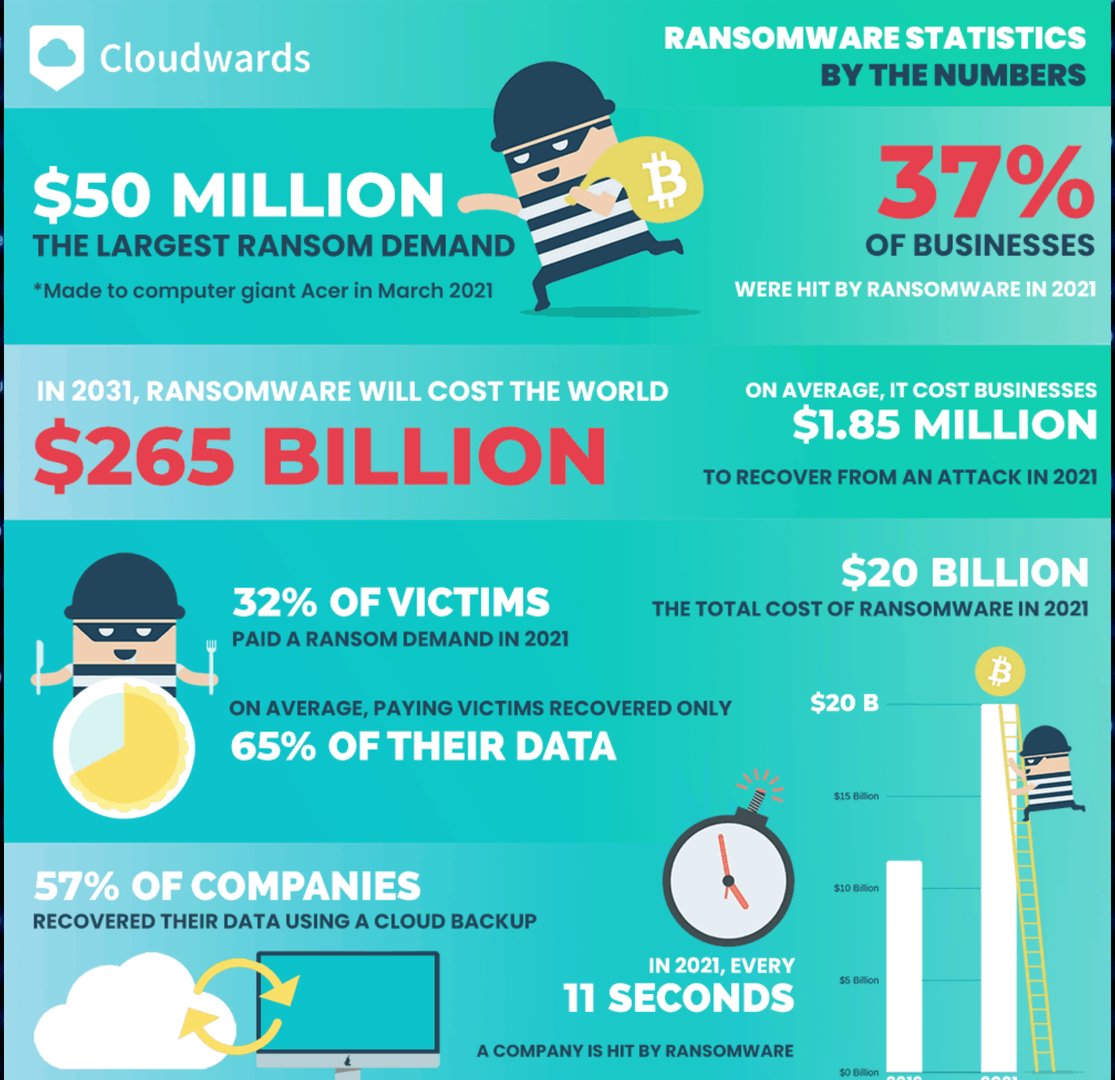
Your files have been Encrypted

To recover your files, send $750,000 worth of Bitcoins to the following Address:

12fjps0932mksJPksd184Mfd01ajsoamf

TIME LEFT

-23:59:28:00



Cloudwards

RANSOMWARE STATISTICS BY THE NUMBERS

$50 MILLION
THE LARGEST RANSOM DEMAND
*Made to computer giant Acer in March 2021

37%
OF BUSINESSES
WERE HIT BY RANSOMWARE IN 2021

IN 2031, RANSOMWARE WILL COST THE WORLD
$265 BILLION

ON AVERAGE, IT COST BUSINESSES
$1.85 MILLION
TO RECOVER FROM AN ATTACK IN 2021

32% OF VICTIMS
PAID A RANSOM DEMAND IN 2021

ON AVERAGE, PAYING VICTIMS RECOVERED ONLY
65% OF THEIR DATA

$20 BILLION
THE TOTAL COST OF RANSOMWARE IN 2021

57% OF COMPANIES
RECOVERED THEIR DATA USING A CLOUD BACKUP

IN 2021, EVERY
11 SECONDS
A COMPANY IS HIT BY RANSOMWARE

Threats need responses…

According to a recent Fortinet whitepaper:

“Prevention can never be 100% effective—advanced threats will always evade prevention-based security. When they do, threats are far harder to detect.”

Thus, ever evolving threats require rapid response capabilities.

Source:
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-hidden-costs-endpoint-security.pdf

Your Objective is to Ensure:

Data Security

- Confidentiality, Integrity

System Availability

- 24x7 access

Regulatory Compliance

How to Gain Total Visibility?

Modern-day security approach

- Integration of
  - People
  - Applied Threat Intelligence
  - SIEM/SOAR/SOC
  - Modern Security Technology

What is Endpoint Detection and Response (EDR?)

Solutions that

- record and store endpoint-system-level behaviors,
- use various data analytics techniques to detect suspicious system behavior,
- integrate with Threat Intelligence,
- block malicious activity,
- provide remediation suggestions or capabilities, and
- ultimately lead to faster restoration of affected systems.

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

What is Endpoint Detection and Response (EDR?)

EDR solutions must provide four primary capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

Endpoint Detection and Response from FFIEC

Procedure 12

Determine the adequacy of security monitoring for the network, critical systems and applications. Also determine whether sufficient controls are in place to protect against malware. Consider the following:

□ …

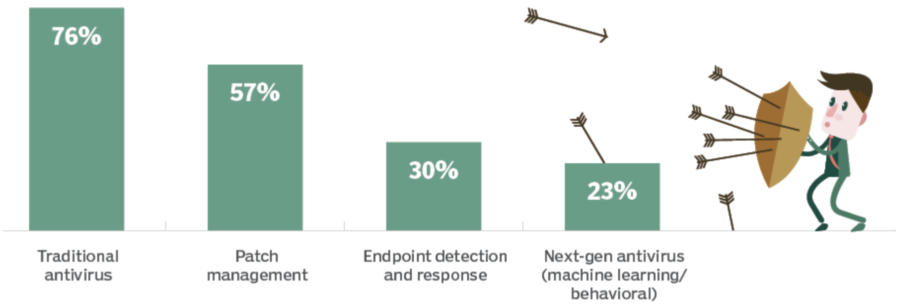
□ *Ability to detect and respond to anomalous activity*

□ …

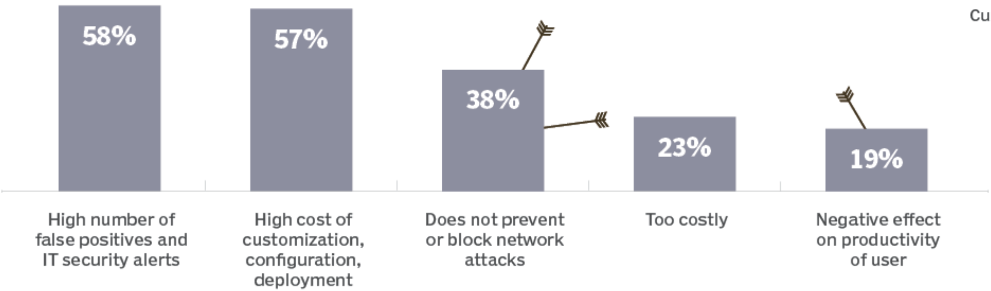
Source: FDIC

Challenges of and approaches to securing endpoints

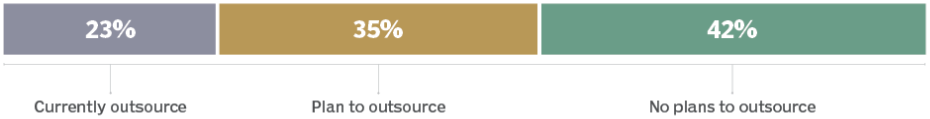
What is your organization using to protect its endpoints?*



What challenges do you face with endpoint detection and response?*

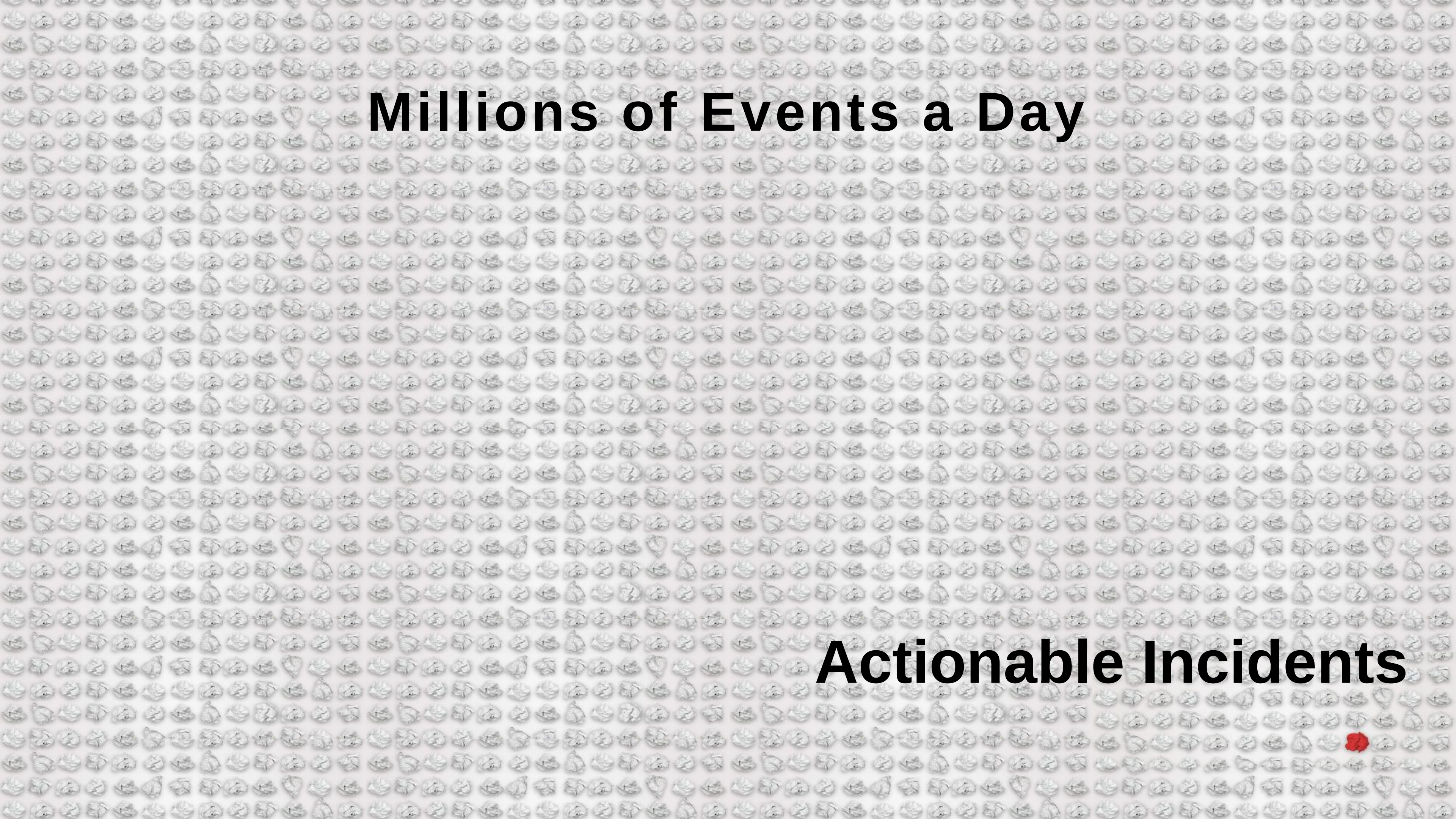


Does your organization outsource or plan to outsource endpoint protection?



Source: https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR

Millions of Events a Day



Actionable Incidents

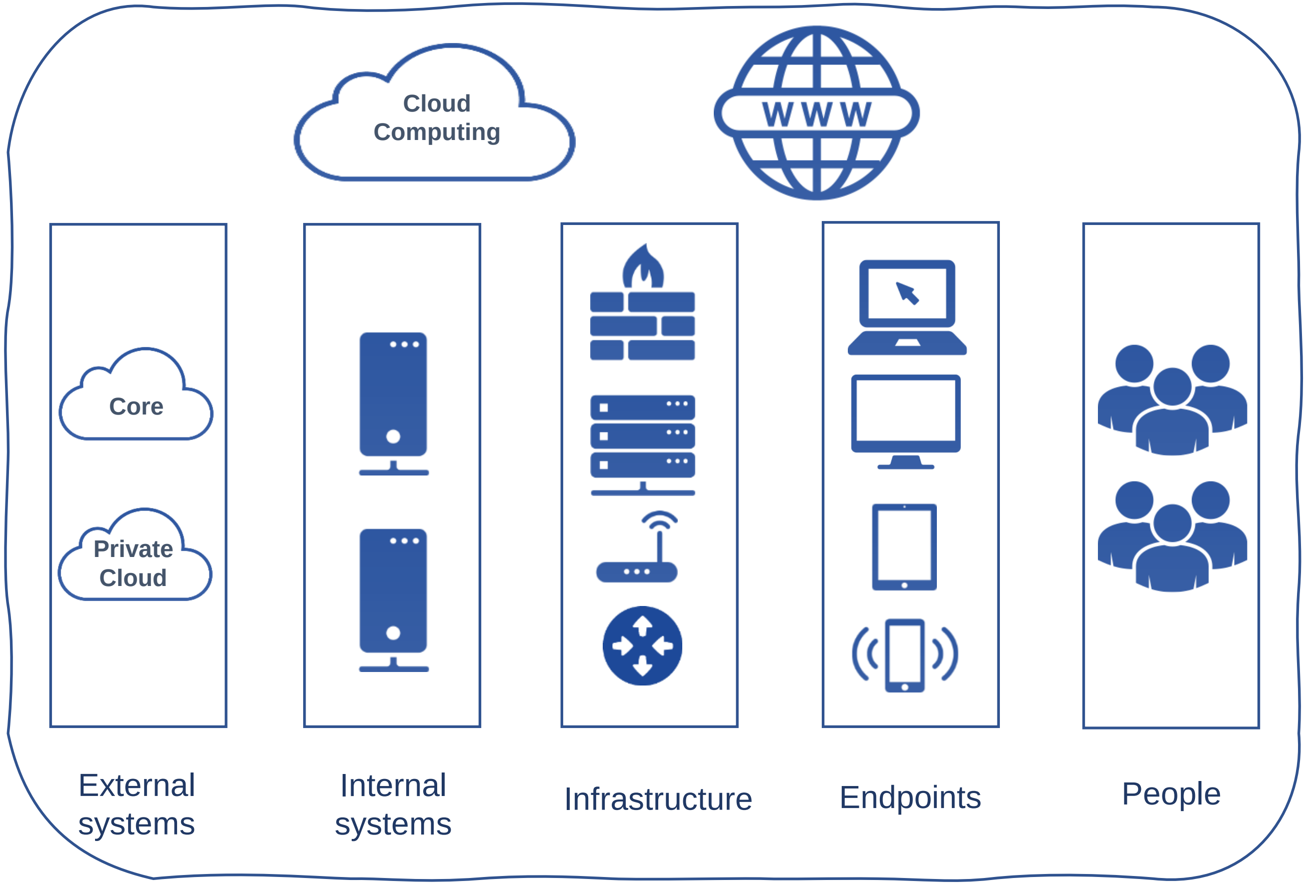
Endpoint Detection and Response

- Rapid notification of endpoint compromise
- Visibility into all your endpoints
- Threat intelligence correlation
- Machine learning detection

✓ Symantec
✓ McAfee
✓ Trend Micro
✓ Microsoft
✓ CrowdStrike
✓ CarbonBlack
✓ Cybereason

Protecting Your Institution's Assets

- Data Security
- 24x7 System Availability
- Regulatory Compliance



Jack Henry - Gladiator® Solutions

IT & Security Services
Total Protect™

Private Cloud Computing
HNS™

Backup & Recovery
Centurion™

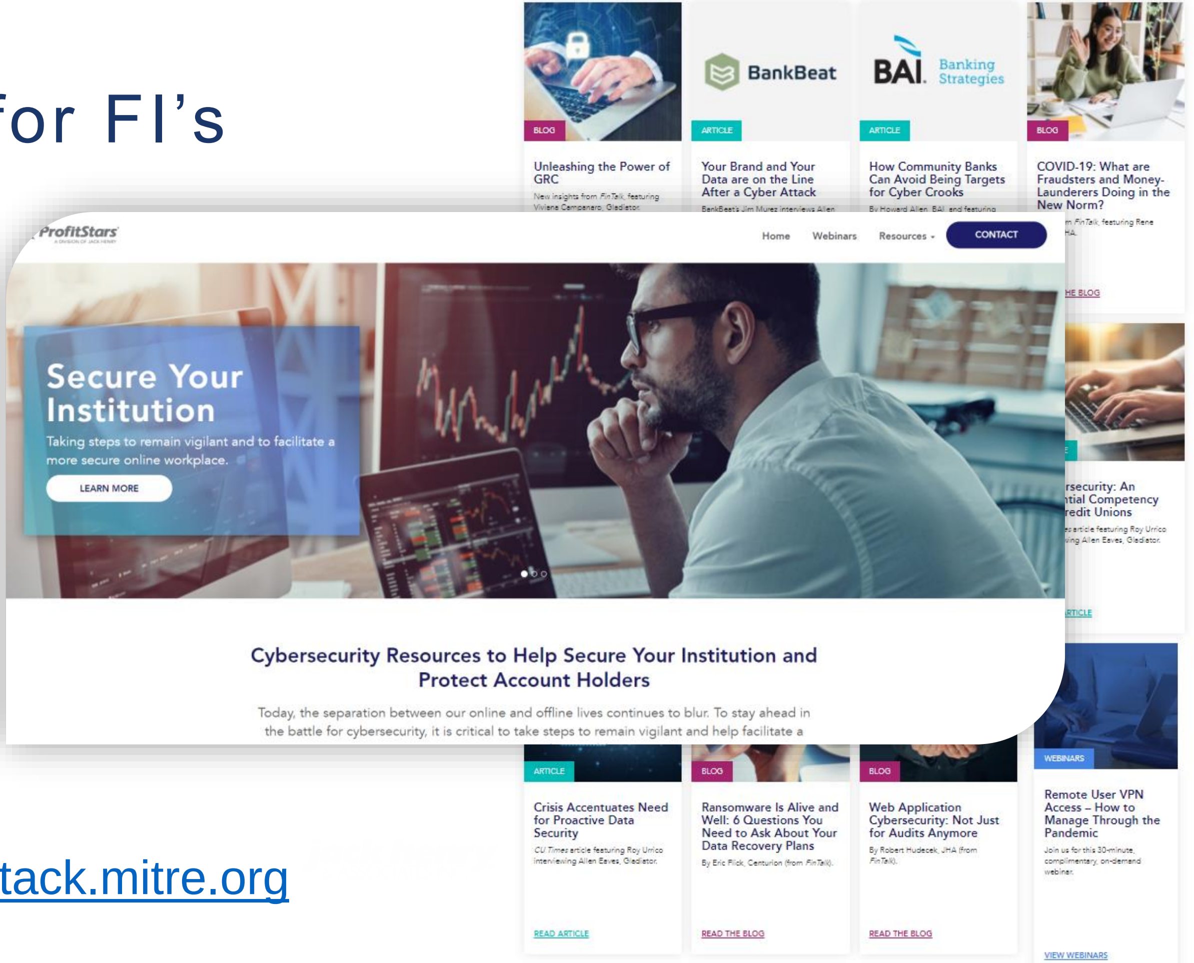
Governance Risk & Compliance
GRC™

Gladiator™ Total Protect Suite

- SIEM Monitoring, Alerting & Reporting
- Firewall Management & Monitoring
- Sandboxing / Early Breach Detection
- DNS Advanced Malware Protection
- Data Loss Prevention (DLP)
- Enterprise Vulnerability Scanning
- OS and Application Patching
- Endpoint Security Management
- Data Backup & Recovery

Resource Center for FI’s

jackhenry.com/cybersavvy



BLOG

Unleashing the Power of GRC

New insights from *FinTalk*, featuring Viviana Campanaro, Gladiator.

BankBeat

ARTICLE

Your Brand and Your Data are on the Line After a Cyber Attack

BankBeat's Jim Murez interviews Allen

BAI Banking Strategies

ARTICLE

How Community Banks Can Avoid Being Targets for Cyber Crooks

By Howard Allen, BAI, and featuring

BLOG

COVID-19: What are Fraudsters and Money-Launderers Doing in the New Norm?

m *FinTalk*, featuring Rene HA.

HE BLOG

ProfitStars

Home Webinars Resources ▾ CONTACT

Secure Your Institution

Taking steps to remain vigilant and to facilitate a more secure online workplace.

LEARN MORE

Cybersecurity Resources to Help Secure Your Institution and Protect Account Holders

Today, the separation between our online and offline lives continues to blur. To stay ahead in the battle for cybersecurity, it is critical to take steps to remain vigilant and help facilitate a

rsecurity: An ntial Competency redit Unions

es article featuring Roy Urrico wing Allen Eaves, Gladiator.

RTICLE

ARTICLE

Crisis Accentuates Need for Proactive Data Security

CU Times article featuring Roy Urrico interviewing Allen Eaves, Gladiator.

READ ARTICLE

BLOG

Ransomware Is Alive and Well: 6 Questions You Need to Ask About Your Data Recovery Plans

By Eric Flick, Centurion (from *FinTalk*).

READ THE BLOG

BLOG

Web Application Cybersecurity: Not Just for Audits Anymore

By Robert Hudecek, JHA (from *FinTalk*).

READ THE BLOG

WEBINARS

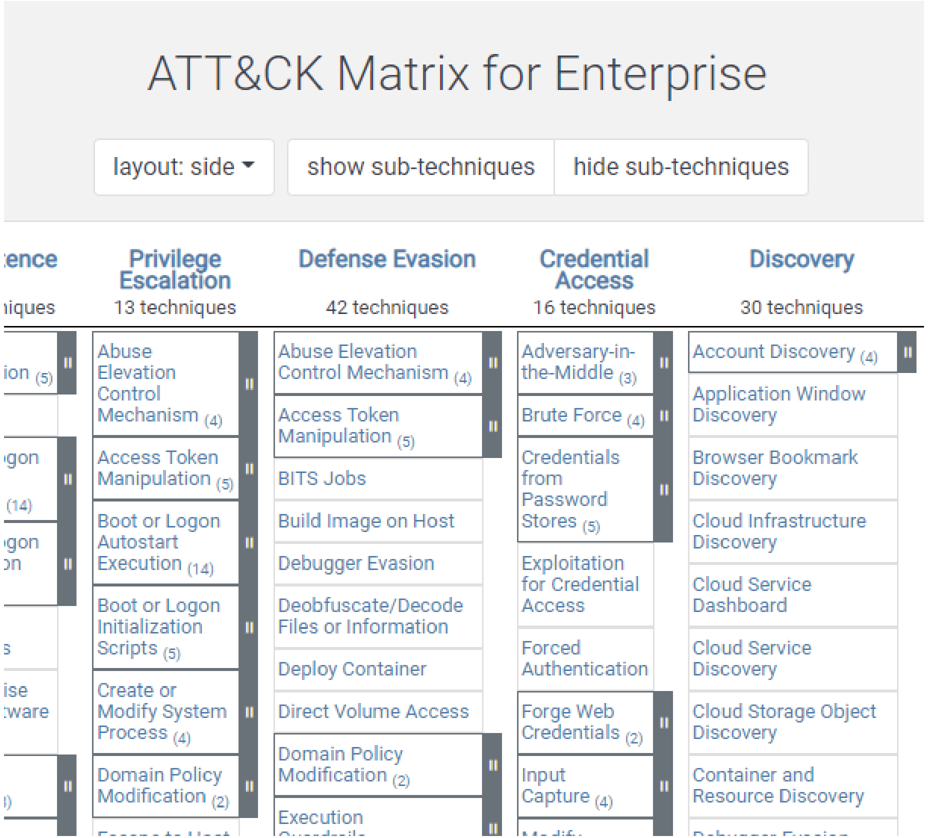
Remote User VPN Access – How to Manage Through the Pandemic

Join us for this 30-minute, complimentary, on-demand webinar.

VIEW WEBINARS

- Blogs
- Whitepapers
- Webinars
- Published articles
- Cybersecurity Forums
- MITRE ATT&CK: https://attack.mitre.org

MITRE ATT&CK Tool



ATT&CK Matrix for Enterprise

layout: side ▾ | show sub-techniques | hide sub-techniques

ence
iques

- ion (5)
- gon (14)
- gon on
- s
- ise tware
-)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution

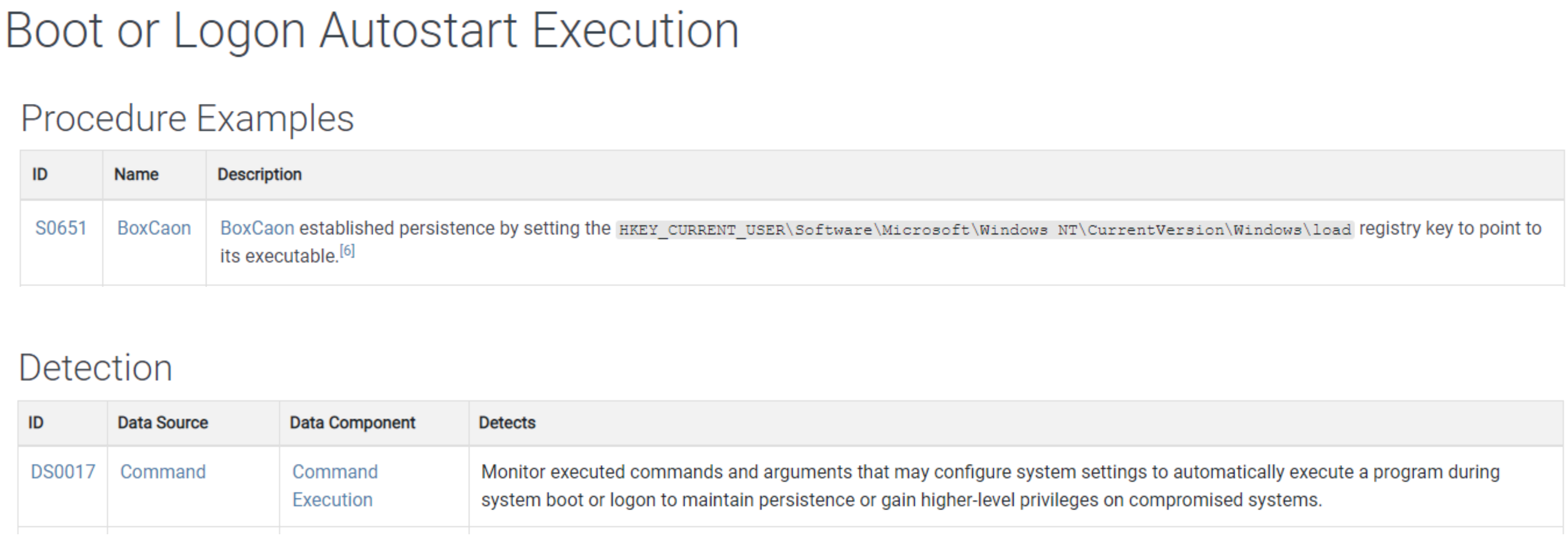
Credential Access
16 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion

MITRE ATT&CK Tool



Boot or Logon Autostart Execution

Procedure Examples

ID	Name	Description
S0651	BoxCaon	BoxCaon established persistence by setting the `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load` registry key to point to its executable.[6]

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.

Thank You!

Scott Dale
scdale@jackhenry.com