



ILTA Webinar: **How Do You Know You** **Haven't Already Been** **Breached?**

May 19, 2021, 2:00 PM – 3:00 PM (EDT)



CORNERSTONE.IT

 **Netsurion®**



Meet Our Team of Experts



Jim Moreo
Principal

Jim.Moreo@cornerstone.it

646-530-8920



Guy Cunningham
Senior VP
of Channel and Alliances

gcunningham@netsurion.com

346-772-2158

Agenda

- Cornerstone Managed Services
- Cybersecurity Challenges
- Cybersecurity & NIST CSF
- Netsurion's Breach Detection
 - Managed Threat Protection
 - EventTracker Enterprise
- Cornerstone + Netsurion Total Solution
- Q & A



Cornerstone.IT Managed Services

Legal IT Focused



24/7 Monitoring



Monthly & Zero-Day
Patching



Vulnerability
Remediation



Daily Health Check
Monthly Security Scans




Support
Services



CORNERSTONE.IT

Cybersecurity Challenges

- 
- 1. Cybersecurity solutions are fragmented.**
 - 2. Cybersecurity is in a constant state of flux.**
 - 3. Cybersecurity expertise is scarce.**



Poll Question #1

Poll Question:

What is the average length of time it takes to identify a successful cyberbreach?

- 35 days
- 113 days
- **207 days**
- 317 days

- (<https://www.ibm.com/security/data-breach>)



NIST Cybersecurity Framework

NIST Cybersecurity Framework functions provides a policy framework of computer security guidance on how businesses can assess and improve their ability to mitigate cyber risk.

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Recover

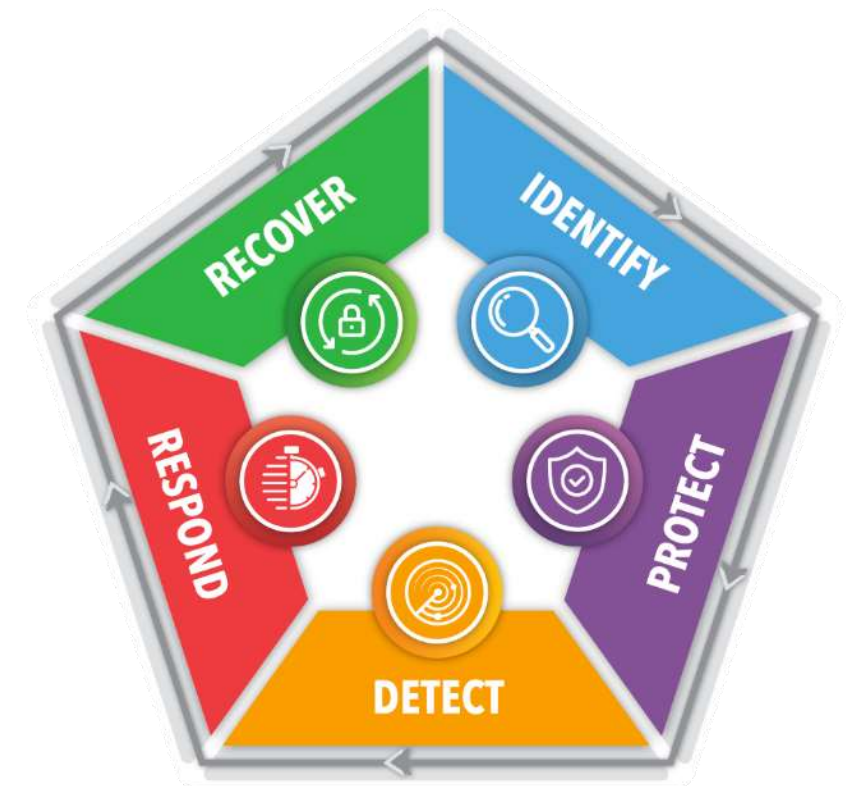
- Recovery Planning
- Improvements
- Communications

Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection and Procedures
- Maintenance
- Protective Technology

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements



NIST Cybersecurity Framework

Identify

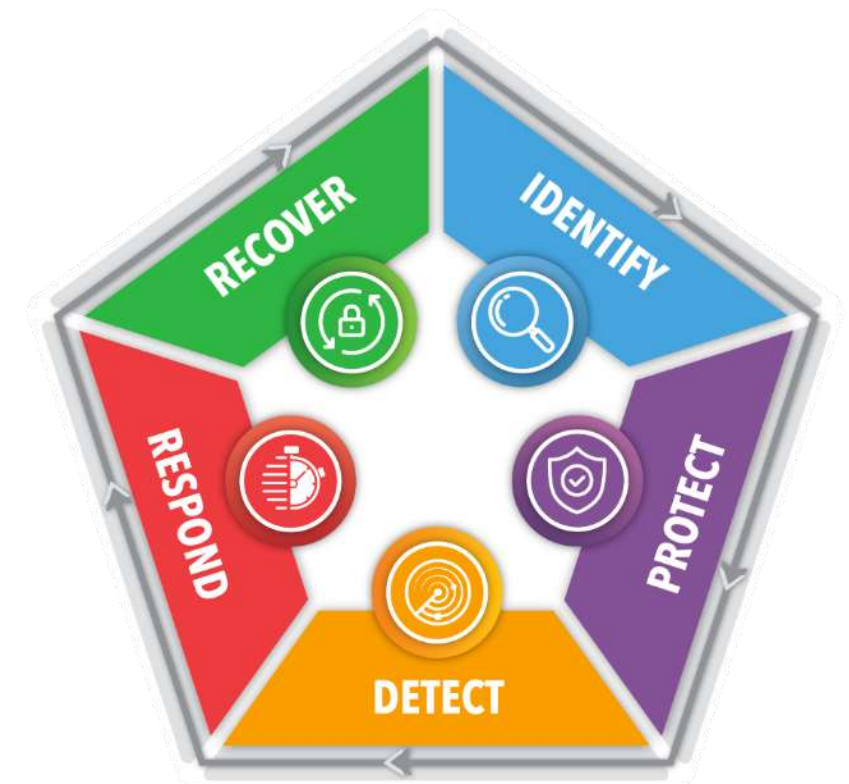
- 24/7 Network Monitoring
- Risk Intelligence Scan and Report
- Monthly Vulnerability Scan
- Hardware & Software Asset Management
- Support Contract Management
- Annual Technology Roadmap
- NIST Policies and Procedures

Respond

- Network Support
- Vulnerability and Breach Remediation

Protect

- Monthly and Zero-Day Patching
- iManage Managed Services
- Citrix Managed Services
- Cisco Infrastructure Managed Services
- Azure Managed Services
- Disaster Recovery Managed Service
- Windows Upgrade Managed Service
- Endpoint Management
- Security Awareness Training
- Machine Learning Antimalware
- Endpoint Encryption
- On-Prem & Cloud Backups
- Disaster Recovery Planning



Identifying the Security Gaps using the CSF Guidance

Aligning the existing network protections against the NIST CSF to understand the gaps in cybersecurity.

Identify

- PC Management
- Network Monitoring
- Vulnerability Scans
- Helpdesk Boards
- Security Awareness Training
- Dark Web Monitoring

Protect

- Patching
- Antivirus & Antimalware
- ESET Endpoint Encryption
- Email Security
- On-Prem Security Appliances & Firewalls
- Web & DNS Protection

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Communications
- Response Planning

Recover

- On-Prem & Cloud Backups
- DR Plan



Filling the Gaps using the CSF

Filling the Detect and Respond CSF Functions with Netsurion EventTracker Enterprise.

Identify

- PC Management
- Network Monitoring
- Vulnerability Scans
- Helpdesk Boards
- Security Awareness Training
- Dark Web Monitoring

Protect

- Patching
- Antivirus & Antimalware
- ESET Endpoint Encryption
- Email Security
- On-Prem Security Appliances & Firewalls
- Web & DNS Protection
- EventTracker EDR

Detect

- Netsurion 24/7 SOC
- Netsurion Managed SIEM
- Netsurion EDR
- Netsurion Threat Intelligence
- Netsurion Machine Learning
- Netsurion Intrusion Detection
- Netsurion Anomalous Logins
- Netsurion Dormant Malware
- Netsurion Communications
- Netsurion Behavior Analysis

Respond

- Netsurion 24/7 SOC
- Netsurion Incident Response
- Netsurion Process Termination
- Netsurion Threat Hunting
- Netsurion Security Reporting
- Netsurion Compliance Reporting

Recover

- Barracuda Backups
- Cybersecurity Insurance
- Disaster Recovery





Poll Question #2

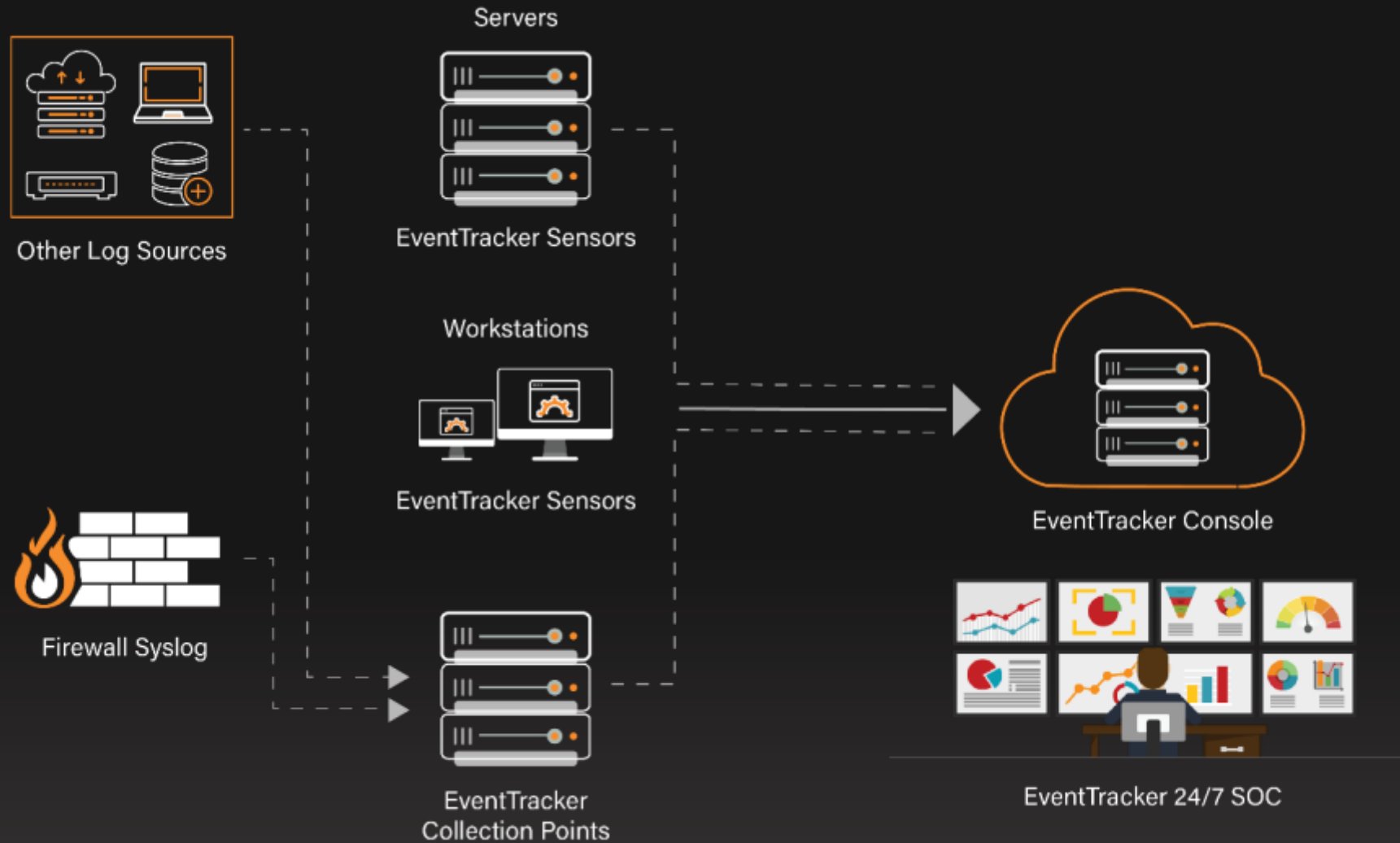
Poll Question:
**How many unique
categories of cyber attack
techniques have been
identified?**

- 122
- 206
- 487
- 623





<https://attack.mitre.org>



EventTracker SIEM Architecture



Cybersecurity Maturity Model

 RESPOND			<ul style="list-style-type: none"> • Basic forensic investigation • Centralized log management 	<ul style="list-style-type: none"> • EDR • Actionable alerts • Incident response playbook 	<ul style="list-style-type: none"> • 24/7 fractional SOC • Integrated SOAR • Response automation – terminate suspicious activity
 DETECT		<ul style="list-style-type: none"> • Mandated compliance log reviews • Conditional alerting • Intrusion Detection System 	<ul style="list-style-type: none"> • SIEM • UEBA • Daily critical observations reports • Network traffic analysis 	<ul style="list-style-type: none"> • Continual SIEM tuning and administration • Threat hunting • Custom dashboards 	<ul style="list-style-type: none"> • 24/7 dedicated SOC
 PREVENT	<ul style="list-style-type: none"> • Anti-virus • Patch management • Next-gen firewall • File integrity monitoring 	<ul style="list-style-type: none"> • Defined user policies, awareness training, certifications • Intrusion prevention system 	<ul style="list-style-type: none"> • Application-level control 	<ul style="list-style-type: none"> • Deep learning endpoint threat prevention on critical devices 	<ul style="list-style-type: none"> • Deep learning endpoint threat prevention fully deployed
 PREDICT	<ul style="list-style-type: none"> • Vulnerability scanning 	<ul style="list-style-type: none"> • Configuration scanning • Advanced vulnerability scanning 	<ul style="list-style-type: none"> • Threat intelligence integration • IT, OT, IoT, and WFH coverage 	<ul style="list-style-type: none"> • Threat research analysts 	<ul style="list-style-type: none"> • Human-supervised machine learning
	OPERATIONAL	EMERGING	FOUNDATIONAL	ADVANCED	OPTIMIZED

Managed Threat Protection Market Challenges



1. **Cybersecurity solutions are fragmented.**

Netsurion's EventTracker Platform and SOC integrate disparate technologies and services allowing our clients to focus on their business.

2. **Cybersecurity is in a constant state of flux.**

Netsurion's managed services continually evolve adding new capabilities automatically to meet our customers changing needs.

3. **Cybersecurity expertise is scarce.**

Netsurion's managed services is delivered by our own experts freeing our customers from the burdens of staffing and 24/7 monitoring.



Poll Question #3

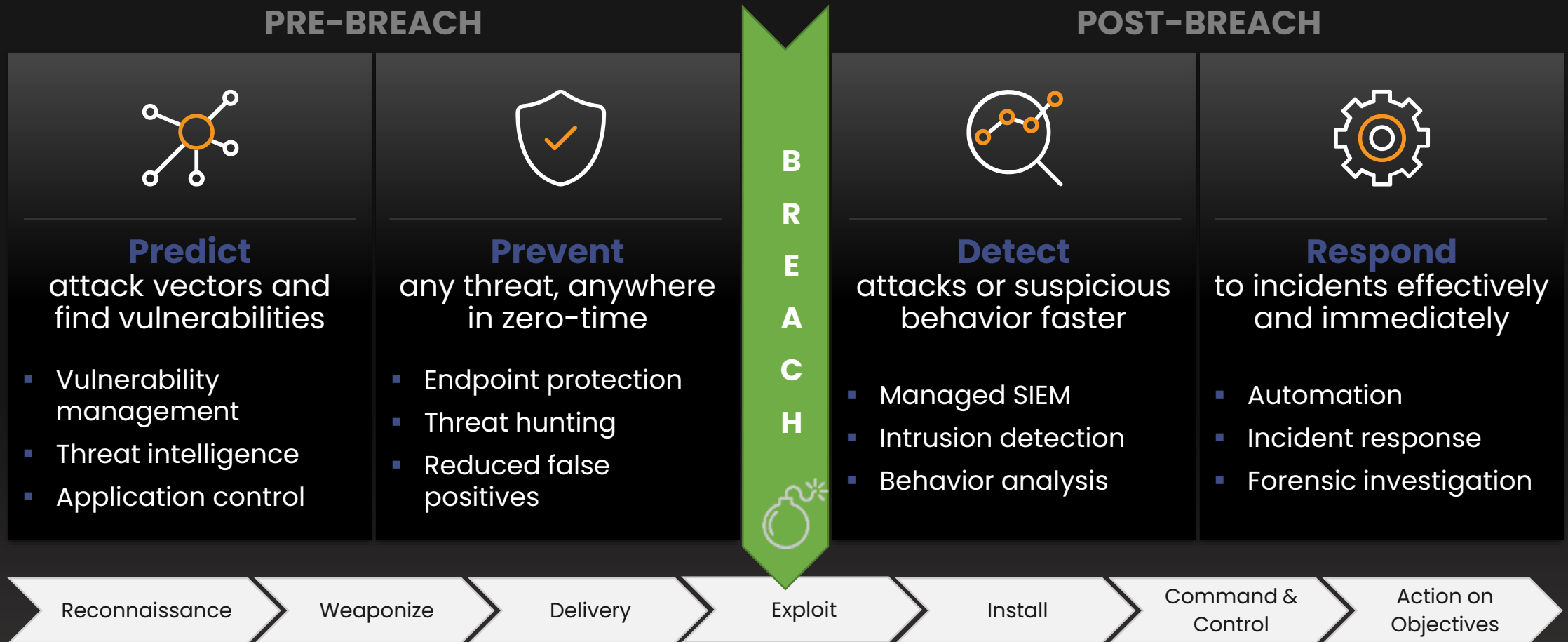
Poll Question:
**How big is the average
ransomware payment?**

- \$32,000
- **\$111,605**
- \$249,000
- \$387,000



<https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/>

Managed Threat Protection is End-to-End Security





Poll Question #4

Poll Question:

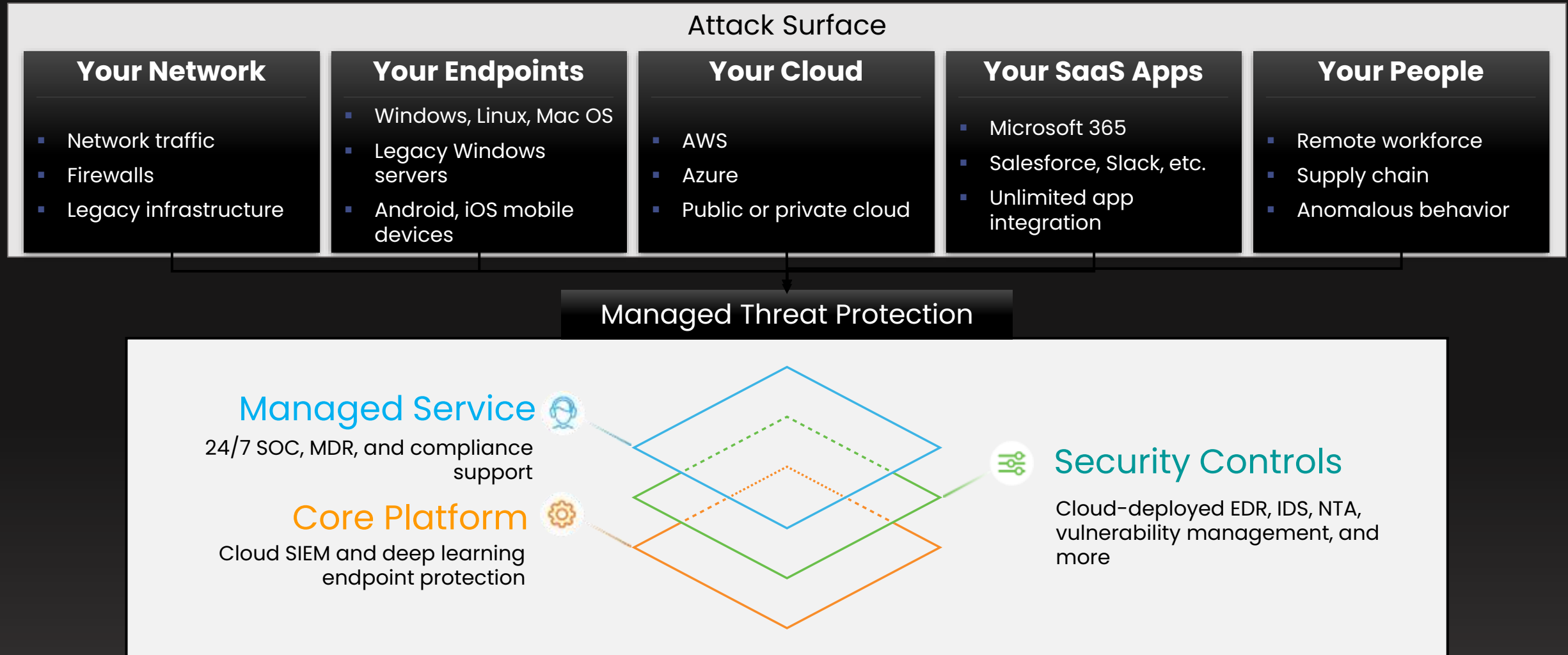
What percentage of successful cyberbreaches start at a laptop or desktop?

- 10%
- 30%
- 50%
- **70%**



- <https://www.rapid7.com/resources/rapid7-efficient-incident-detection-investigation-saves-money/>

Protect Your Entire Attack Surface



Fully-Staffed SOC



Client Team Lead: Critical observations report, monthly review and planning

Security Analysts: Threat hunting, incident response

Client Coordinator: Meetings and action item management



COMPLIANCE TEAM

- CISSPs
- PCI DSS
- ISO 20001
- NIST, CSF, GDPR, etc.



MONITORING TEAM

- 24/7 monitoring
- Incident escalation



TECH STACK TEAM

- Servers
- Cloud
- Firewalls
- Applications



INTELLIGENCE TEAM

- Log knowledge
- Security intelligence
- Log formats, definitions
- Use cases



PLATFORM TEAM

- EventTracker experts
- Software engineering
- Agile development



We've got you
covered.



Q & A

Thank you!

Get our Remote Desktop Pro solution
on the Azure Marketplace



CORNERSTONE.IT

Call for more information: 646-530-8920

Ask a question via email:

- Jim.Moreo@Cornerstone.IT
- GCunningham@netsurion.com

Netsurion®

