CrowdStrike eBook

THE SECRET TO CYBERSECURITY FOR SMALL BUSINESSES

Learn how the right combination of technology, people and processes can protect your business against advanced cyberthreats

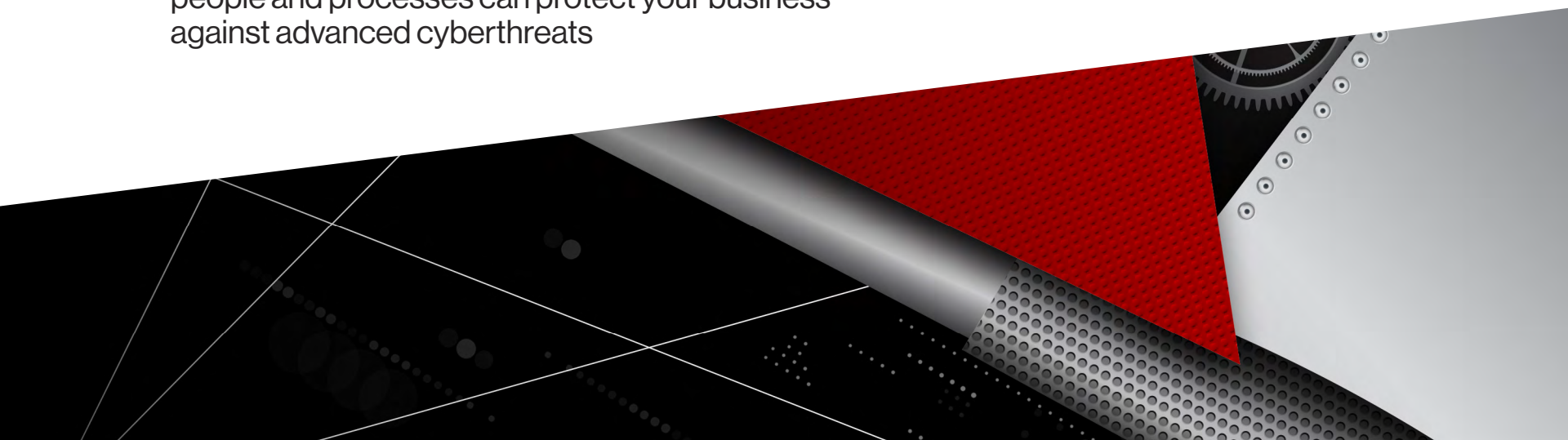


TABLE OF CONTENTS

CYBERATTACKS AGAINST SMALL BUSINESSES ARE ON THE RISE

- **Ransomware:** A type of malware that disables access to your system and data until a ransom is paid
- **Extortion:** An attacker extracts and then threatens to expose sensitive information on the internet unless the victim makes an extortion payment
- **Data theft:** An attacker extracts and then sells valuable employee data or intellectual property

What do a lawn care company, an independent insurance broker and a boutique clothing store have in common? They're all small businesses at risk of data breaches.

While much of the reporting on cyberattacks focuses on large companies, the truth is that small businesses are not immune. According to Ponemon Institute, 63% of small and medium-sized businesses worldwide experienced a data breach during fiscal year 2019, up from 54% just two years earlier[1].

CYBERCRIMINALS DEPLOY A RANGE OF TACTICS

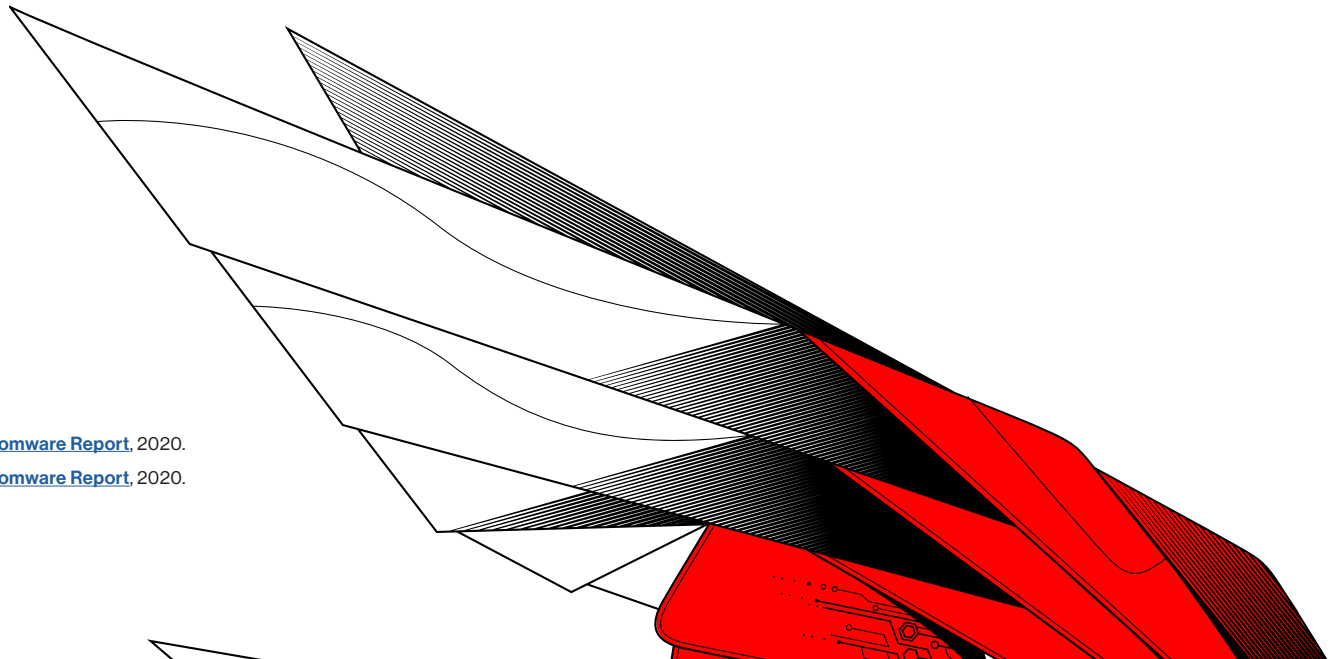
Cyberattacks come in many forms, from ransomware and cyber extortion, to theft of sensitive data such as personal information about employees or intellectual property. While many small businesses are familiar with malware and may have installed antivirus to combat these kinds of attacks, the reality is that the threat landscape is much more complex than it used to be. Today, many cyberattacks gain a foothold without deploying malware. According to CrowdStrike's 2020 Global Threat Report, malware-free attacks are up from 49% to 60% as a proportion of all attacks between 2018 and 2020[2].

1 Ponemon Institute, **2019 Global State of Cybersecurity in Small and Medium-Sized Businesses**, October 2019.

2 CrowdStrike, **2020 Global Threat Report**, 2020.

60% OF MANAGED SERVICE PROVIDERS REPORTED RANSOMWARE ATTACKS AGAINST SMALL AND MEDIUM BUSINESSES IN 2020[3]

Ransomware continues to be a major concern for small companies. When cybercriminals hold critical data for ransom, your business is effectively shut down — customers can't place new orders, suppliers can't deliver materials and employees can't access the information they need to do their jobs. While the average ransom payment that hackers request from small businesses is $5,600, the total cost is often much higher. When you factor in costs of downtime, legal services and other aspects of responding to a breach, estimated damages average 50 times more than the payment[4].



3 Datto, **Datto's Global State of the Channel Ransomware Report**, 2020.

4 Datto, **Datto's Global State of the Channel Ransomware Report**, 2020.

BUST MYTHS, THEN CYBERCRIMINALS

When large corporations like LinkedIn, eBay and Accellion endure cyberattacks, the event makes headlines. The same isn't always true for small businesses. In the absence of media attention, it's easy for misinformation to spread — including the idea that small businesses are not exposed to the same cyberthreats as large corporations. So, let's dispel some common myths.

TOP 5 CYBERSECURITY MISCONCEPTIONS FOR SMALL BUSINESSES

1. CYBERATTACKS COME FROM BASEMENT HACKERS

The idea that hackers are lone attackers working with amateur setups might be easier to stomach than the reality: they are highly organized, disciplined and specialized cybercriminals who act fast. Recently, well-funded, highly organized criminal groups have been more relentless and sophisticated than ever, deploying a range of new tactics, techniques and procedures[5]. For instance, ransomware as a service (RaaS) provides cybercriminals with a ready-made kit to use malicious code that locks you out of your system.

2. CYBERCRIMINALS DON'T CARE ABOUT THE DATA I HAVE

Some small businesses may think they fly under the radar of cybercriminals since they have less data than large corporations. However, most small and medium-sized businesses (63%) experienced a data breach in 2019[6]. Because small businesses typically don't have the sophisticated technology and dedicated security teams of a large enterprise, they can be an easier target for attackers.

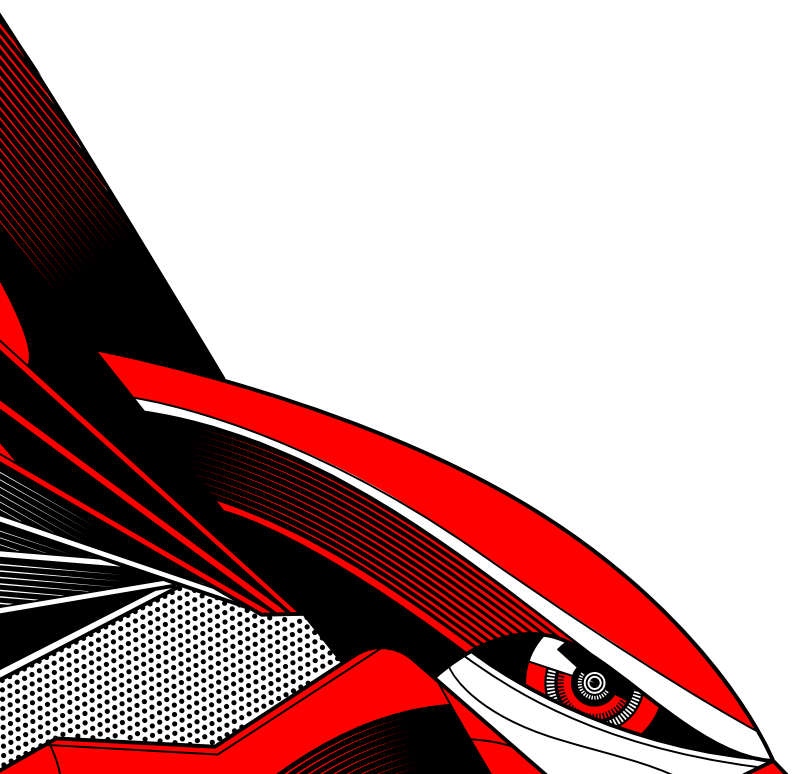
---

5 CrowdStrike, **2020 Global Threat Report**, 2020.

6 Ponemon Institute, **2019 Global State of Cybersecurity in Small and Medium-Sized Businesses**, October 2019.

3. I HAVE ANTIVIRUS AND A FIREWALL, SO I'M PROTECTED FROM CYBERTHREATS

This is only partly true. Legacy technologies are incapable of detecting and stopping the sophisticated techniques employed by today's attackers. Further, while cybersecurity technology is a major component in protecting small businesses, it requires mature processes in place and capable people to run them. For 24/7 security operations, a small business would need roughly five full-time security analysts, at least, to keep up with emerging threats — but few small businesses are staffed at this level, indicating that many are underprepared and over-reliant on their technology platforms.



4. I'LL KNOW IF I'VE BEEN BREACHED

Cybercriminals are experts at camouflage. The longer they can stay inside your system, the more damage they can potentially do. When a breach does happen, it often takes just a few hours. It can occur at 3 a.m. on a holiday when the office is closed, or over a long weekend when staffing is low. But on average, it takes 79 days to discover a data breach[7], which is far too late to prevent damage to your organization.

5. MY COMPANY WILL BE ABLE TO BOUNCE BACK AFTER AN ATTACK

By 2025, global cybercrime is expected to reach a staggering $10.5 trillion, representing the greatest transfer of wealth in history[8]. The average ransom requested from small businesses was $5,600[9], but that's just the beginning. Factoring in business downtime, decreased profitability, legal fees and more, a severe data breach or attack might be the final straw that forces some small businesses to shut down.

In the real world, believing in these myths can lead to costly, detrimental mistakes.

---

7 CrowdStrike, **CrowdStrike Services Cyber Front Lines Report**, December 2020.

8 Cybercrime Magazine, **Cybercrime to cost the world $10.5 trillion annually by 2025**, November 2020.

9 Datto, **Datto's Global State of the Channel Ransomware Report**, 2020.

LAW FIRM DATA FOR SALE ON THE DARK WEB

Target: Mid-sized law firm

Attack: Malware with persistence mechanisms

Damage: Network access and client case data for sale on the dark web

PHISHING USES EMAIL, SMS, PHONE OR SOCIAL MEDIA TO ENTICE A VICTIM TO SHARE SENSITIVE INFORMATION — SUCH AS PASSWORDS OR ACCOUNT NUMBERS — OR DOWNLOAD A MALICIOUS FILE THAT WILL INSTALL VIRUSES.

It's not every day the FBI calls your office. For a mid-sized law firm, the news was grim. The FBI was calling to notify the company that access to its network of 750 endpoints, including some of its high-profile client case data, was for sale on the dark web. The law firm was unsure when and how the cyberattackers had gained access, but compromised credentials or phishing were likely avenues. Once inside the network, the cybercriminals set up persistence mechanisms to infect the systems more easily with malware, then exfiltrated sensitive client data.

The law firm had been compromised even though it was running a legacy security solution and had one team member dedicated to security. But realistically, one security staffer can only keep an eye on things during work hours, leaving lots of time for the attacker to gain a foothold undetected. With no prior remediation experience and no threat hunting capabilities, the law firm was caught off guard against such an attack.

All told, the law firm spent over $100,000 on a forensic incident response, providing the FBI, internal counsel and insurance provider with information on how access was gained, what data was exfiltrated or destroyed, and what adversary artifacts still remained. An engagement of this scale typically takes multiple months and many hours spent pulling logs and coordinating with an incident response firm.

UTILITY NARROWLY ESCAPES RANSOMWARE

Target: Mid-sized utility

Attack: Emotet and TrickBot malware

Damage: Ransomware attempts on critical server infrastructure

EMOTET IS A SOPHISTICATED BANKING TROJAN THAT EVADES SIGNATURE-BASED DETECTION, IS PERSISTENT, AND INCLUDES SPREADER MODULES THAT HELP IT PROPAGATE.

TRICKBOT IS AN ADVANCED AND PERSISTENT MODULAR TROJAN THAT HAS INFECTED UPWARD OF ONE MILLION SYSTEMS WORLDWIDE.

What's the worst that could happen through a phishing campaign? One mid-sized commercial utility company will say that its biggest issue is dealing with ransomware attempts. The company's two-person IT and security team noticed suspicious activity in their environment one Friday and reached out to CrowdStrike to help identify the behavior.

After deploying CrowdStrike Falcon Prevent™ next-generation antivirus, the company gained visibility across its 500 endpoints and found roughly 250 detections of Emotet and TrickBot behavior. This criminal "tag team" of Emotet and TrickBot is known for its ability to quickly infect networks with malware. As Emotet, a banking trojan, moves through a system, it employs TrickBot to steal money by accessing online bank and PayPal accounts. With the intrusion under control, the company engaged CrowdStrike's Falcon Complete experts to return all affected systems to a safe state. Thanks to quick intervention, Emotet and TrickBot were stopped before they could execute ransomware on critical server infrastructure.

Although the utility company had a legacy antivirus solution in place, it still had limited security resources and IT that left it vulnerable to attacks. Without 24/7 protection, remediation experience, and a formal plan for incident response, the company was almost at the mercy of a malware duo.

GUARD YOUR BUSINESS WITH A SOLID SECURITY POSTURE

Relying on antivirus software and firewalls is simply not enough. Today's cybercriminals are too sophisticated, fast and evolving for legacy measures. It takes a combination of technology, people and processes to identify and react to threats in near real time, 24/7.

- **Threat hunting:** Proactively searching for cyberthreats that are lurking undetected in a network
- **Investigation:** Monitoring and prioritizing security alerts to determine which require action
- **Response:** Containing and eradicating threats before they can inflict damage to your organization
- **Next-generation protection:** A cloud-managed solution that leverages machine learning to stop known threats and provides complete visibility so teams can respond to emerging threats

Figure 1. Four main components of a solid security posture

TECHNOLOGY: NEXT-GENERATION PROTECTION

LEGACY ANTIVIRUS HAS BEEN OUTSMARTED

LEGACY ANTIVIRUS SOFTWARE RELIES ON SIGNATURE-BASED DETECTION TO IDENTIFY MALWARE. SIGNATURES REQUIRE CONSTANT UPDATING, AND SIMPLY CAN'T KEEP UP WITH THE RAPID PACE OF NEW MALWARE DEVELOPMENT.

A modern technology platform is the foundation of your solid security posture. It's much more advanced than your typical legacy solutions — it's built to block malware and malicious behavior as it occurs, without cumbersome signature updates or performance-draining system scans.

Intelligent detection: A modern cybersecurity platform leverages artificial intelligence and machine learning to detect predatory behavior in real time before attackers wreak havoc on your network.

Cloud-based architecture: Backed by the cloud, a modern cybersecurity platform has the ability to scale and update its intelligent models to keep up with fast-moving, constantly evolving attackers. It also means there's no hardware or additional software to install, and the platform is continuously tuned to ensure you're always prepared to stop the latest threats.

The power of the crowd: It's one thing to stop today's threats, but it's quite another to learn from cyberthreat behavior and proactively prepare for tomorrow. A modern cloud-native cybersecurity platform has the capacity to learn from millions of encounters with cyberattackers encountered over months and years, and ensure that all organizations, from the very smallest to the largest, have the same excellent protection.

PEOPLE AND PROCESSES: THREAT HUNTING

ARTIFICIAL INTELLIGENCE STILL NEEDS HUMANS

EACH NEW GENERATION OF SECURITY TECHNOLOGY CAN DETECT A GREATER NUMBER OF ADVANCED THREATS — BUT THE MOST EFFECTIVE DETECTION ENGINE IS STILL THE HUMAN BRAIN.

An automated technology platform isn't always enough to stop determined, creative attackers. Cyberattackers are well aware of how security technologies detect their malicious behavior, so they continuously adapt. Using new techniques, they evade detection and blend in with normal day-to-day administrative activity. Any security plan that relies entirely on technology to detect threats is risking a high-impact, silent failure. You need determined, creative people hunting for stealthy activity in a sea of security data.

Threat hunting: The task is identifying the malicious activity. When attackers are constantly shifting to outmaneuver your technology platform, it's up to threat hunters to see through the camouflage and uncover the faint tracks left by advanced attacks. Threat hunters possess years of experience and valuable intuition to understand how attackers operate and predict their next move. And threat hunters operate 24/7/365, because attackers don't take breaks or holidays.

Information gathering: Once suspicious behavior is detected, threat hunters gather and analyze as much information as possible to discern the cybercriminal's methods and goals, and then send their insights upstream to alert the investigation team.

Future preparation: Using the insights they've learned from continuous hunting and encounters with today's sophisticated attackers, threat hunters make predictions on future attacker behavior to help you reduce vulnerabilities in your network and better prepare for uncovering the threats of tomorrow.

PEOPLE AND PROCESSES: INVESTIGATION

CAN'T STOP, WON'T STOP
INVESTIGATING AN ALERT CONTINUES UNTIL EITHER THE ACTIVITY IS DEEMED BENIGN OR A COMPLETE PICTURE OF THE MALICIOUS BEHAVIOR HAS BEEN CREATED.

Sometimes a security alert represents a real threat to your network. Sometimes it's benign activity or a false alarm. Whether alerts come from your technology platform or your team of threat hunters, each one must be investigated. It's the only way to know for sure if the alert indicates signs of attack or nothing at all.

Alert prioritization: A central task for investigators is to identify and prioritize the most urgent alerts. They're experts at looking at the context of an alert to determine which data, assets or infrastructure the incident could affect. Every alert should be reviewed. While low-severity alerts are easy to ignore and are often benign, they can provide early insights pointing to the first stages of emerging threats. Identifying threats early gives defenders the critical time they need to respond in time to stop a breach.

Alert analysis: Understanding the full context of a security alert requires asking all of the right questions and leveraging your security platform to obtain answers. Investigators must identify what happened, which systems were affected and what damage was done. Only then can you mount an effective response.

Feedback loop: Ideally, your investigation team has the bandwidth to learn from the malware it has blocked and suggest measures to prevent future attacks. Even when everything goes right — or wrong — there's still an opportunity to learn. Investigating how malware entered your organization, and whether it was the first or last stage of the attack, provides critical information to ensure you've addressed the core threat so you can bolster your defenses for the future.

PEOPLE AND PROCESSES: RESPONSE

HACKS ARE HAPPENING FASTER

CYBERCRIMINALS ONLY NEED A FEW HOURS TO GO FROM INTRUSION TO MAJOR OUTBREAK.

ACT FAST WITH THE 1-10-60 RULE

IF YOU'RE GOING TO BE EFFECTIVE AT AVOIDING BREACHES, STRIVE FOR THIS BEST PRACTICE:

1 MINUTE TO DETECT A THREAT

10 MINUTES TO INVESTIGATE AND TRIAGE

60 MINUTES TO CONTAIN AND REMEDIATE

Cybercriminals act fast. You need an actionable response process in place to enable your security team to act swiftly and shut down threats as soon as they are identified. Having a response plan in place ensures your team can operate in a repeatable manner and prioritize their time. Remember the 1-10-60 rule: It should take one minute to detect, 10 minutes to investigate and 60 minutes to remediate.

Fast action: A tested, thorough response plan standardizes, centralizes and automates as much information as possible from your technology platform, your threat hunters and your investigation team so you can act quickly and respond effectively. Too often, organizations respond to threats too late and with blunt force (such replacing entire systems).

Surgical remediation: When it comes to cleaning up after an incident, organizations often use cumbersome techniques such as reimaging and completely rebuilding affected systems, which can be more damaging than the incident itself. This process is slow, expensive and has a high impact on your end users. Remediating an incident should be surgical, with minimal effect on the rest of your network. Whether you're resetting passwords, cleaning up file systems or removing malware, the objective is to remove any compromised aspects with care, limiting the possibility of collateral damage.

Protection optimization: Containing and eradicating threats is only half the battle. Your security and operations staff should garner new knowledge with every incident response to prepare for next time.

FALCON COMPLETE™ PROVIDES FULL PROTECTION 24/7

The days of relying on antivirus and firewalls to protect your organization are over. An effective cyber defense requires a solid security foundation built on world-class technology, people and processes. The CrowdStrike Falcon Complete managed endpoint security solution delivers all three — cloud-native endpoint protection, a team of battle-hardened threat hunters, and expert security analysts running proven, established processes to see, stop and prevent determined attackers. Gain peace of mind with managed endpoint protection delivered immediately — and skip the burden of building and managing it yourself.

Stop threats: Falcon Complete keeps pace with modern cyberattackers to stop them in their tracks. With 24/7 alert and incident handling, plus a full team of threat hunters, investigators and responders, Falcon Complete has you covered from alert to remediation.

Save money: Bring on the security team you need, without the cost of in-house staffing. And with complete protection, you'll reduce end-user downtime and business disruptions. Falcon Complete is also backed by the industry's most comprehensive breach prevention warranty.

Hit the ground running: With CrowdStrike's proven onboarding program, most customers are up and fully operational in just a few days. CrowdStrike ensures your environment is always up-to-date so you don't need to spend any effort managing agents, signatures or policies. With a fully optimized environment, you're prepared to combat the latest threats.

CASE STUDY: GREENHILL ADVISES GLOBAL FINANCE CLIENTS WHILE PROTECTING DATA WITH LEADING SECURITY

ESTIMATED REDUCTION IN ALERTS

ANNUAL SAVINGS

ENDPOINTS

Greenhill is a global independent investment bank that has grown its services and footprint since its founding in 1996 and remains mid-market in size, a factor that presents security challenges, according to CIO John Shaffer.

"It's important to be prepared in an ever-changing threat landscape populated by threat actors plus staff who bring their own devices and connect them from home," Shaffer explains. "That presents a major challenge for our team to ensure that our data remains our data, and to affirm our employees' home networks do not become a bridge for getting into our corporate network."

Greenhill leveraged CrowdStrike technology to protect its endpoints, coupled with Falcon Complete to achieve its vision. Falcon Complete experts assist Greenhill with all security tasks, including deploying and managing the Falcon platform from the initial onboarding and configuration stages, to prevention health checks, maintenance and operations, incident triage and hands-on remote remediation.

"Adding managed services to our CrowdStrike deployment made it even more valuable," Shaffer says. "Falcon Complete helped Greenhill to improve our security posture, shrink the time needed to respond to threats, and eliminate the need to reimage systems during remediation."

"All the behind-the-scenes security CrowdStrike does to make sure our environment is safe means we can spend time on projects that are more meaningful and more effective for our end users," he continues. "In acting as an extension of our security team by providing resources and expertise we do not have internally, CrowdStrike has given us peace of mind we otherwise would not have."

TECHNOLOGY, PEOPLE AND PROCESSES ALL IN ONE

Learn more about **Falcon Complete** for fast, easy protection against all threats.

CrowdStrike Falcon Complete provides a comprehensive managed endpoint protection solution, to help organizations achieve continuous response. It delivers unparalleled security by augmenting the CrowdStrike Falcon® platform with the expertise and 24/7 engagement of the Falcon Complete team. The team manages and actively monitors the Falcon platform, remotely remediating incidents continuously as they occur. Falcon Complete enables organizations with effective and mature endpoint security without the difficulty, burden and costs, and backs it with a Breach Prevention Warranty of up to $1M.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike:
We stop breaches.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**