ActZero

CXO INSIGHT

Blueprint for Ransomware Defense

A foundational cybersecurity plan for SMEs

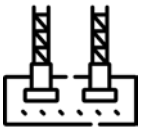
Ransomware is no longer just a financial crime; it is an urgent security risk that threatens businesses, and government agencies around the world. Small- and medium-sized enterprises (SMEs) have been increasingly hard hit by ransomware. Accenture's 2019 Cost of Cybercrime Study, for example, revealed that "43% of cyber attacks target small businesses, but only 14% are prepared to defend themselves."

In response to this growing threat, the Ransomware Task Force (RTF) was formed in December 2020 to find effective new methods of countering the ransomware threat. Operating under the Institute for Security and Technology (IST), the RTF launched it's seminal report in April of 2021. Within that report, Action 3.1.1 – of particular note to SMEs – called for the cybersecurity community to "develop a clear, actionable framework for ransomware mitigation, response, and recovery". The Blueprint for Ransomware Defense Working Group – *in which ActZero played a significant contributing role* – was formed shortly thereafter with the specific goal of developing a set of actionable and easily achievable "Safeguards". This new **Blueprint for Ransomware Defense** and it accompanying resources was launched in August 2022.

What's in the Blueprint?

Aimed at SMEs that have small IT teams with limited cybersecurity expertise, the Blueprint provides a short list of recommended defensive actions that can be taken to combat ransomware and other common cyber attacks. The 40 easily-implementable Safeguards provide "essential cyber hygiene" – the protective controls and foundational capabilities necessary to help defend against general, non-targeted attacks.

Control Types



14 Foundational Controls
Practices enterprises must implement to effectively undertake other cybersecurity actions.

26 Actionable Controls
Practices that increase an enterprise's cybersecurity posture.

Functions

Identify	Protect	Detect (not included)	Respond	Recover

SMEs should implement as many of the Blueprint Safeguards as possible. Even partial implementation is an important step in increasing your cybersecurity, and it lays the groundwork for more advanced capabilities like detecting and rapidly responding to threats that have evaded protective measures.

How can ActZero help?

As noted, the 'Detect' function, was not included in the RTF Blueprint. Why? Because this critical function is almost impossible for SMEs to do alone. Being able to detect and stop adversaries who bypassed protective measures is key to avoiding ransomware, and implementing a Managed Detection and Response (MDR) service is the best way to accomplish this goal.

Having played and integral role within the Working Group, ActZero is well-positioned to help SMEs not only understand, plan for, and track implementation of the 40 Safeguards, but complete the resilience effort by adding our advanced threat intelligence, machine learning models and human threat hunting to help detect, contain and respond to any threats that evade your protections.

With ActZero you can:

- **Better understand your current Ransomware Readiness Posture**

  It's hard to be successful on a journey when you're not exactly sure where you are now. ActZero can help you quickly assess your current status against the Blueprint, and identify the gaps.

- **Get advice on how to close your gaps**

  Let our team of experts review your reports, answer strategic, technical and implementation questions, and provide you with the clear and prioritized guidance needed to progress your cybersecurity goals.

- **Track successful completion to the Blueprint in our Maturity Model**

  Need help tracking your success? ActZero's maturity model allows you to track and upload evidence of controls completion. We give you an easy way to pull reports for executives and auditors.

- **Secure the additional detection capabilities needed to level-up your protections**

  ActZero's AI and ML intelligently pinpoint threats to endpoints, network, mobile and cloud that have evaded your defenses. Our Threat Hunters waste less time filtering noise, and spend more time advising you on the immediate actions to be taken.

- **Leverage your cyber readiness to lower your cyber insurance premiums**

  Insurers require enterprises to better understand, implement, and demonstrate cyber risk management practices before qualifying. ActZero helps customers meet these goals, and **obtain up to 20% off their cyber insurance premiums***

Let our FREE ransomware readiness assessment show you what you're missing by emulating a complete ransomware attack operation on your organization to identify key vulnerabilities, help you understand the Blueprint for Ransomware Defense, and show you how we'll close the gaps and limit any operational disruptions.

*Conditions apply